BlackBerry Enterprise Server for Microsoft Exchange

Version: 5.0
Service Pack: 4

Security Technical Overview

Published: 2014-01-17
SWD-20140117135425071

Contents

New in this release

1

The table lists the updated security features for the BlackBerry Enterprise Server 5.0 SP4 that are described in this document.

Feature	Description
Transcoder encryption	If your organization uses a transcoder to provide an additional level of encryption for data that is sent to and from smartphones, you can specify whether the BlackBerry transport layer encryption or the transcoder encryption is applied last if the smartphone supports the option to apply the transcoder encryption after the transport layer encryption.

Overview

2

BlackBerry Enterprise Solution security

The BlackBerry Enterprise Solution consists of various products and components that are designed to extend your organization's communication methods to BlackBerry devices. The BlackBerry Enterprise Solution is designed to help protect data that is in transit at all points between a device and the BlackBerry Enterprise Server. To help protect data that is in transit over the wireless network, the BlackBerry Enterprise Server and device use symmetric key cryptography to encrypt the data sent between them. The BlackBerry Enterprise Solution is designed to prevent third parties, including wireless service providers, from accessing your organization's potentially sensitive information in a decrypted format.

The BlackBerry Enterprise Solution uses confidentiality, integrity, and authenticity, which are principles for information security, to help protect your organization from data loss or alteration.

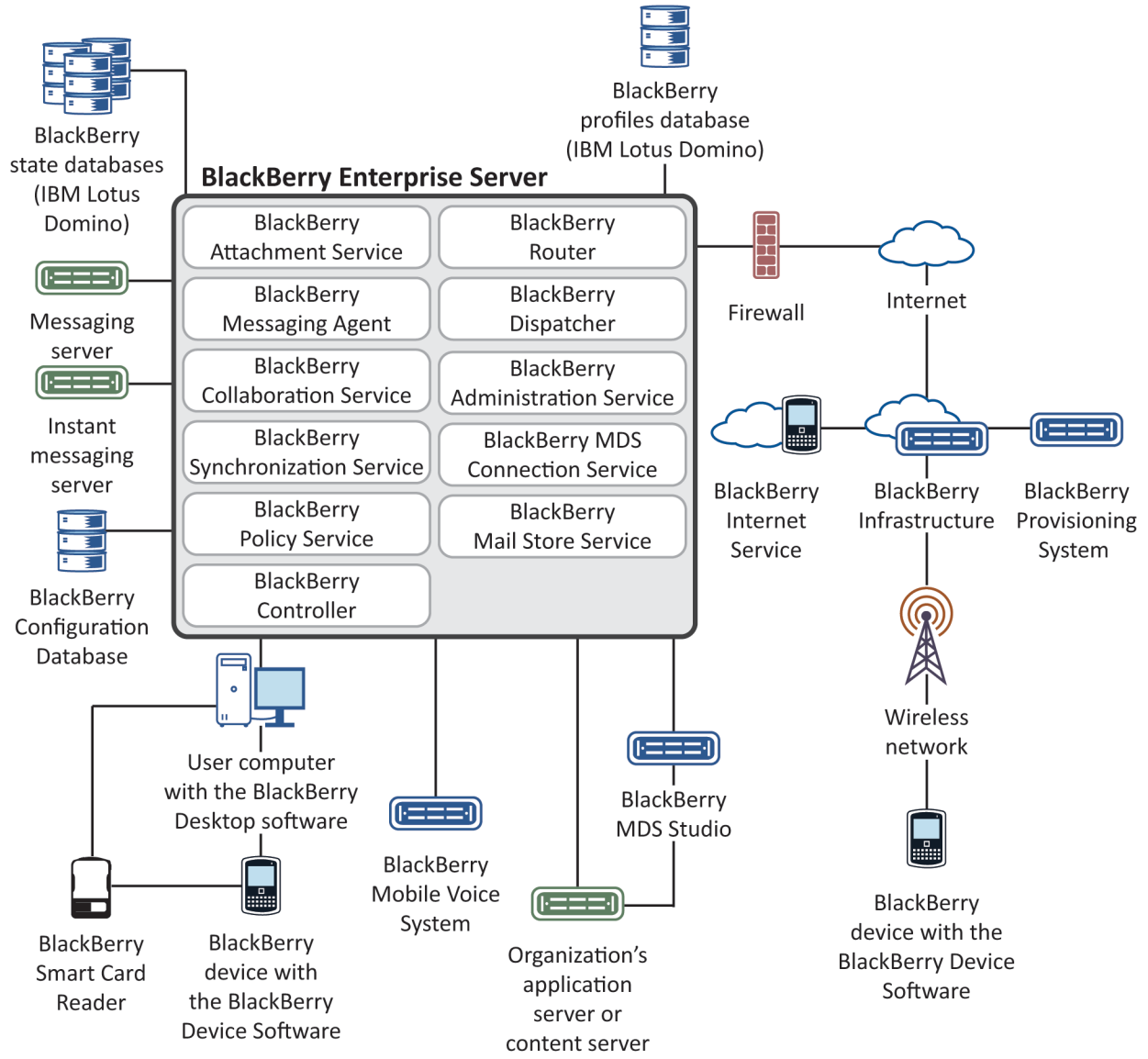
Principles	Description
confidentiality	The BlackBerry Enterprise Solution uses symmetric key cryptography to help make sure that only intended recipients can view the contents of email messages.
integrity	The BlackBerry Enterprise Solution uses symmetric key cryptography to help protect every email message that the device sends and to help prevent third parties from decrypting or altering the message data. Only the BlackBerry Enterprise Server and the device know the value of the keys that they use to encrypt messages and recognize the format of a decrypted and decompressed message. The BlackBerry Enterprise Server or the device rejects a message automatically if it is not encrypted with keys that they recognize as valid.
authenticity	Before the BlackBerry Enterprise Server sends data to the device, the device authenticates with the BlackBerry Enterprise Server to prove that the device knows the device transport key that is used to encrypt data.

Security features of the BlackBerry Enterprise Solution

Feature	Description
data protection	The BlackBerry Enterprise Solution is designed to protect data that is in transit between the BlackBerry Enterprise Server and a BlackBerry device and data that is in transit between your organization's messaging server and the email application on a user's computer. The BlackBerry Enterprise Solution encrypts data that is stored on the device and in the BlackBerry Configuration Database. To help protect data that is stored on the device, you can require a user to authenticate to the device using a password, a smart card, or both.
encryption key protection	The device is designed to protect the encryption keys that are stored on the device. The device encrypts the encryption keys when the device is locked.
control of device connections	The BlackBerry Enterprise Solution is designed to control the following connections: • connections using Bluetooth technology to and from the device • connections from a Wi-Fi enabled device to enterprise Wi-Fi networks The BlackBerry Enterprise Solution is designed to control which devices can connect to the BlackBerry Enterprise Server.
control of the behavior of the device and BlackBerry Desktop Software	To control the behavior of the device and BlackBerry Desktop Software, you can send IT administration commands, IT policies, and application control policies to the device. You can use IT administration commands, IT policies, and application control policies to perform the following actions: • You can send IT administration commands to lock the device, permanently delete work data, permanently delete user information and application data, and return the device settings to the default values. • You can send an IT policy to a device to change security settings. You can use the IT policy to enforce the device password and BlackBerry Smart Card Reader password. • You can send an application control policy to a device to control whether third-party applications are available and can connect to the device and whether third-party applications or add-on applications developed by Research In Motion can access work data.

Architecture: BlackBerry Enterprise Solution

The BlackBerry Enterprise Solution consists of various components that permit you to extend your organization's communication methods to BlackBerry devices.



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service is a BlackBerry Enterprise Server component that connects to the BlackBerry Configuration Database. You can use the BlackBerry Administration Service to manage BlackBerry Enterprise Server components, user accounts, and features for a device.

Component	Description
BlackBerry Attachment Service	The BlackBerry Attachment Service is a BlackBerry Enterprise Server component that converts supported message attachments into a format that the user can view on a device.
BlackBerry Collaboration Service	The BlackBerry Collaboration Service is a BlackBerry Enterprise Server component that provides a connection between your organization's instant messaging server and the collaboration client on a device.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains configuration information that BlackBerry Enterprise Server components use. The BlackBerry Configuration Database stores the following information: • details about the connection from a BlackBerry Enterprise Server to the wireless network • contact list • address mappings between PINs and email addresses for BlackBerry MDS Connection Service push features • read-only copies of device transport keys, which encrypt the message keys that encrypt data that the BlackBerry Enterprise Server and a device send between each other
BlackBerry Controller	The BlackBerry Controller is a BlackBerry Enterprise Server component that monitors other BlackBerry Enterprise Server components and restarts them if they stop responding.
BlackBerry Desktop Software	The BlackBerry Desktop Software is an integrated suite of applications that a user installs on the user's computer. It manages the association between a device and the email account, synchronizes organizer data, calendar entries, and inboxes, and permits the user to download applications and BlackBerry Device Software updates to a device.
BlackBerry device	A device provides the user with access to BlackBerry services such as messaging and browsing.
BlackBerry Device Software	The BlackBerry Device Software consists of applications on a device that permit the user to send and receive email messages, PIN messages, and text messages; manage calendar entries; and so on.
BlackBerry Dispatcher	The BlackBerry Dispatcher is a BlackBerry Enterprise Server component that compresses and encrypts all data that a device sends and receives. The BlackBerry Dispatcher sends the data through the BlackBerry Router, to and from the wireless network.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server consists of various components that process, route, compress, encrypt, and send data over the wireless network to a device. The BlackBerry Enterprise Server is designed to open a two-way connection that is highly secure between the user's email account and the device. The

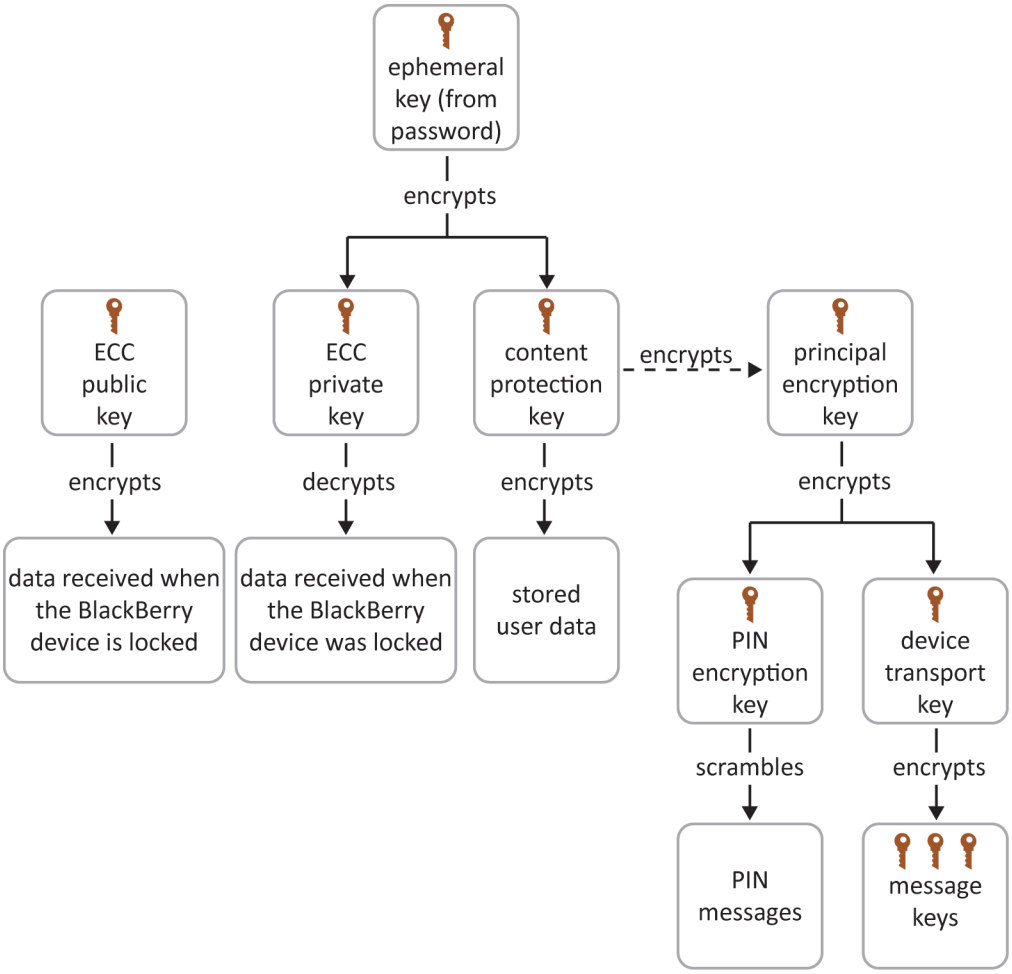
Component	Description
	BlackBerry Enterprise Server uses the connection to send email messages inside your organization's firewall.
BlackBerry Infrastructure	The BlackBerry Infrastructure is designed to manage the wireless transport of messages between the wireless network and a device.
BlackBerry Internet Service	The BlackBerry Internet Service provides a subscriber with messaging service and access to Internet content on a device.
BlackBerry Mail Store Service	The BlackBerry Mail Store Service connects to the messaging servers in your organization's environment and retrieves the contact information that the BlackBerry Administration Service requires to search for user accounts on the messaging servers.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service is a BlackBerry Enterprise Server component that permits the user to access web content, the Internet, or your organization's intranet from a device. The BlackBerry MDS Connection Service also permits applications on a device to connect to your organization's application servers or content servers to retrieve application data and updates.
BlackBerry Messaging Agent	The BlackBerry Messaging Agent is a BlackBerry Enterprise Server component that connects to your organization's messaging server to provide messaging services, calendar management, contact lookups, attachment viewing, and attachment downloading. The BlackBerry Messaging Agent also generates device transport keys and acts as a gateway for the BlackBerry Synchronization Service to access organizer data on the messaging server. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and user mailboxes.
BlackBerry Mobile Voice System	The BlackBerry MVS integrates your organization's PBX phone system with the BlackBerry Enterprise Server to extend desk phone features to a device.
BlackBerry Policy Service	The BlackBerry Policy Service is a BlackBerry Enterprise Server component that sends IT policies and IT administration commands and provisions service books. The BlackBerry Policy Service sends service books to configure settings for features and components on a device.
BlackBerry profiles database	The BlackBerry profiles database is an IBM Domino database that the BlackBerry Enterprise Server for IBM Domino uses to store configuration data for the user account.
BlackBerry Provisioning System	The BlackBerry Provisioning System is designed to permit wireless service providers to configure and manage BlackBerry services for their subscribers. A wireless service provider can assign, activate, deactivate, suspend, and resume BlackBerry services and check the current status of service requests for a device on the wireless network.

Component	Description
BlackBerry Router	The BlackBerry Router is a BlackBerry Enterprise Server component that connects to the wireless network to send data to and from a device. The BlackBerry Router also sends data over your organization's network to a device that is connected to a computer that hosts the BlackBerry Device Manager.
BlackBerry Smart Card Reader	The BlackBerry Smart Card Reader controls access to your organization's sensitive communications using Bluetooth technology and the latest encryption technologies. The BlackBerry Smart Card Reader permits an organization to use two-factor authentication.
BlackBerry state databases	The BlackBerry state databases are Domino databases that the BlackBerry Enterprise Server for IBM Domino uses to store data that associates email messages that a device sends or receives to corresponding messages in the user's email application. The data in the BlackBerry state databases supports features such as email message reconciliation, email message forwarding, email message filing, and replying with text.
BlackBerry Synchronization Service	The BlackBerry Synchronization Service is a BlackBerry Enterprise Server component that synchronizes organizer data between a device and your organization's messaging server over the wireless network.
instant messaging server	The instant messaging server stores instant messaging accounts.
messaging server	The messaging server receives, sends, and stores all email messages.
organization's application server or content server	Your organization's application server or content server provides push applications and intranet content that the BlackBerry MDS Services use to install on a device.

Keys on a device

3

The BlackBerry Enterprise Solution generates keys that are designed to protect the data that is stored on a BlackBerry device and the data that the device and BlackBerry Enterprise Server send between each other.



Key	Description
content protection key	The content protection key encrypts user data on the device when the device is locked.
device transport key	The device transport key encrypts the message keys.
ECC private key	The ECC private key decrypts data when the user unlocks the device.
ECC public key	The ECC public key encrypts the stored data that the device receives when the device is locked.
ephemeral key	The ephemeral key encrypts the ECC public key, ECC private key, and content protection key on the device.
PIN encryption key	The PIN encryption key scrambles PIN messages.
principal encryption key	If you or a user turns on content protection, the principal encryption key encrypts the device transport key and PIN encryption key that is specific to your organization when the device is locked.
message keys	The message keys encrypt data sent to and from the device.

Enforcing the FIPS mode of operation on a device

FIPS are computer-system standards that were developed by the United States federal government and specify requirements for security algorithms. The BlackBerry device uses the AES cipher-based DRBG as the FIPS-validated random source. The device uses the FIPS 186-2 DSA PRNG as the non-FIPS random source. You can configure the Enforce FIPS Mode of Operation IT policy rule to specify whether a device must operate in FIPS mode.

You can also configure the Force Cryptographic Power Analysis Protection IT policy rule to specify whether a device must use algorithms that are protected against cryptographic power analysis (if available).

If the Enforce FIPS Mode of Operation IT policy rule or the Force Cryptographic Power Analysis Protection IT policy rule is enabled, the device displays this information in the Security Status Information section, in the Security options on the device.

For more information about using IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*. For more information about the DRBG function, see *NIST Special Publication 800-90*. For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*.

Device transport keys

The device transport key encrypts the message keys that help protect the data sent between a BlackBerry Enterprise Server and BlackBerry device. The BlackBerry Enterprise Server and device generate the device transport key when a user activates the BlackBerry device.

The BlackBerry Enterprise Server and device do not send the device transport key over the wireless network when they generate the device transport key or when they exchange messages.

The BlackBerry Enterprise Solution is designed so that only the BlackBerry Enterprise Server and device know the value of the device transport key. The BlackBerry Enterprise Server and device reject a data packet if they do not recognize the format of a data packet or do not recognize the device transport key that protects the data packet.

States for device transport keys

The BlackBerry Enterprise Solution generates device transport keys on a regular basis so that a potentially malicious user cannot access all data sent between a BlackBerry Enterprise Server and BlackBerry device if that user compromises a device transport key. As the BlackBerry Enterprise Solution generates device transport keys, the device transport keys change state from pending to current to previous.

State	Description
pending	A pending device transport key is the device transport key that the BlackBerry Enterprise Solution generates to replace the current device transport key. If the user generates the device transport key using the BlackBerry Desktop Software, the BlackBerry Desktop Software sends the pending device transport key to the device when the user connects the device to the computer. The messaging environment and BlackBerry Configuration Database store the pending device transport key.
current	A current device transport key is the device transport key that the device currently uses to encrypt and decrypt message keys.
previous	A previous device transport key is the device transport key that the device used before the BlackBerry Enterprise Solution generated the current device transport key. The device stores previous device transport keys in flash memory for 7 days. The device stores previous device transport keys so that a user can decrypt messages even after the user generates a new device transport key while messages are queued.

State	Description
	The messaging server and BlackBerry Configuration Database store the previous device transport key that the BlackBerry Enterprise Server and device used most recently. A potentially malicious user cannot use the previous device transport key to learn the currrent device transport key. The BlackBerry Enterprise Server and device discard the key pair after they generate the device transport key. If a potentially malicious user compromises both the static private key and ephemeral private key for a device transport key, other device transport keys that the BlackBerry Enterprise Server and device generate are not compromised.

Where the BlackBerry Enterprise Solution stores device transport keys

The BlackBerry Enterprise Solution stores current, pending, and previous device transport keys in the BlackBerry Configuration Database, in the messaging environment, and on each BlackBerry device.

A device stores the device transport keys in a key store database in flash memory. The key store database is designed to prevent a potentially malicious user from copying the device transport keys to a computer by trying to back up the device transport keys. A potentially malicious user cannot extract key data from flash memory.

To avoid compromising the device transport keys that are stored in the BlackBerry Configuration Database or in the messaging environment, you must protect the BlackBerry Configuration Database and the storage location of the device transport key in the messaging environment.

Messaging environment	Storage location on the messaging environment
IBM Domino	BlackBerry profiles database
Microsoft Exchange	mailbox of the email application on the user's computer
Novell GroupWise	—

Where the BlackBerry Enterprise Server stores device transport keys in a Microsoft Exchange environment

In a Microsoft Exchange environment, the BlackBerry Enterprise Server stores the device transport keys in a hidden folder that is named BlackBerryHandheldInfo. The BlackBerryHandheldInfo folder is located in a root folder of the mailbox for the user account on the Microsoft Exchange Server. The BlackBerryHandheldInfo folder stores the following data:

- message of class `RIM.BlackBerry.Handheld.Config` that contains the user's configuration information, including the device transport key

- device transport keys in binary form with tags that indicate whether the status of the device transport keys is pending (0x6002 tag), current (0x6003 tag), or previous (0x6004 tag)

Where the BlackBerry Enterprise Server stores device transport keys in an IBM Domino environment

In an IBM Domino environment, the BlackBerry Enterprise Server stores the device transport keys in a Domino database that is named BlackBerryProfiles.nsf. The BlackBerry profiles database contains configuration information for every user account that exists in the Data directory. The BlackBerry profiles database stores an account record that contains the RIMCurrentEncryptionKeyText field, RIMPendingEncryptionKeyText field, and RIMPreviousEncryptionKeyText field. The fields stores the device transport keys for every user account in a hexadecimal string using alphanumeric characters.

Generating device transport keys

Generating the first device transport key for a device during the activation process

If a user connects a BlackBerry device to a computer for the first time and activates the device, the BlackBerry Desktop Software generates the device transport key and sends it to the device and messaging server.

If a user activates the device over the wireless network, the BlackBerry Enterprise Server and device negotiate to select the strongest algorithm that they both support (either AES or Triple DES) and use that algorithm to generate a device transport key. To generate public keys for key rollover on the device and create a strong, cryptographically protected connection between the BlackBerry Enterprise Server and device, the BlackBerry Enterprise Solution uses the SPEKE authentication method and the activation password for the device.

For more information about the SPEKE authentication method, visit http://standards.ieee.org/ to read *Password-Based Public Key Cryptography (P1363.2)*.

Security characteristics for generating the first device transport key

Characteristics	Description
authentication and integrity	The wireless activation process verifies that only a user with the correct activation password can activate a BlackBerry device that you associate with a BlackBerry Enterprise Server.
prevention of offline dictionary attacks	The wireless activation process is designed so that a potentially malicious user cannot determine a user's password by viewing the protocol packets that the BlackBerry Enterprise Server and device send between each other.
prevention of online dictionary attacks	The wireless activation process is designed so that the BlackBerry Enterprise Server prevents a potentially malicious user from activating a device if that user types an incorrect activation password more than five times.

Characteristics	Description
long-term public keys exchanged	The wireless activation process verifies that the BlackBerry Enterprise Server and device can exchange the device transport key in a manner that is designed to be highly secure when they generate a new device transport key.

Generating subsequent device transport keys for a device

By default, the BlackBerry Enterprise Server and BlackBerry device generate subsequent device transport keys every 30 days. If a pending device transport key exists and a user connects a device to a computer, the current device transport key on the device becomes the previous device transport key and the pending device transport key becomes the current device transport key. If no pending device transport key exists, you, the user, or the BlackBerry Desktop Software can generate a device transport key.

The BlackBerry Enterprise Server and device generate the device transport key using existing long-term public keys and the ECMQV key exchange algorithm to negotiate a device transport key. This method is designed so that a potentially malicious user is unable to calculate the device transport key. The BlackBerry Enterprise Server and device discard the key pair after they generate the device transport key.

For more information about the ECMQV key exchange algorithm, see *NIST: Special Publication 800-56: Recommendation on Key Establishment schemes, Draft 2.0* and the *Guide to Elliptic Curve Cryptography*.

Security characteristics for generating subsequent device transport keys

Characteristics	Description
authentication	Authentication means that only a BlackBerry device that a user authenticates with or a BlackBerry Enterprise Server can generate subsequent device transport keys. Authentication is designed so that a potentially malicious user cannot use another device to impersonate an activated device and generate a device transport key.
password independent	Password independent means that the user does not require an activation password and you do not have to perform any actions when you or a user generates a subsequent device transport key.
flexible initiation	Flexible initiation means that you or a user can generate a subsequent device transport key at any time.
PFS	PFS means that subsequent device transport keys are independent of previous device transport keys. A device transport key does not help the potentially malicious user decrypt data that another device transport key protects.

Generating a device transport key manually

To generate a device transport key on an activated BlackBerry device, a user can click Regenerate Encryption Key, in the device options, in the security options. The device sends the request to generate a device transport key to the BlackBerry Enterprise Server over the wireless network.

A user can also generate a device transport key using the BlackBerry Desktop Manager. By default, the BlackBerry Enterprise Server sends a request to the BlackBerry Desktop Manager every 30 days to prompt the user to generate a new device transport key on the device, even if the user chooses to generate the device transport key manually using the BlackBerry Desktop Manager.

You can use the BlackBerry Administration Service to start the process to generate a new device transport key.

Data flow: Generating a device transport key using BlackBerry Desktop Software version 4.0 or later

In BlackBerry Desktop Software version 4.0 or later, the process to generate a device transport key uses the current time and cursor movements as the seeds to generate random data.

To generate the device transport key, the BlackBerry Desktop Software performs the following actions:

1. prompts the user to move the cursor
2. uses the srand function of the C programming language to examine the lowest 12 bits of the x and y co-ordinates of the new cursor location

   If the bits are different from the previous sample, the BlackBerry Desktop Software stores the bits, which generates 3 bytes of randomness. If the bits are the same as the bits in the previous sample, the BlackBerry Desktop Software does not store any bits.
3. uses the srand function to examine the next bits, after the srand function waited for a random interval between 50 milliseconds and 150 milliseconds

   The srand function continues to wait for random intervals and examine bits until the BlackBerry Desktop Software stores 384 bytes of randomness.
4. retrieves 384 bytes of randomness from the Microsoft Cryptographic API, for a total of 768 bytes
5. hashes the 384 bytes of randomness from the cursor co-ordinates and the 384 bytes of randomness from the Microsoft Cryptographic API with SHA-512 to produce 512 bits of data
6. frees the computer memory that is associated with the unused bits
7. generates the device transport key using the first 256 bits of data if the BlackBerry Desktop Software supports AES encryption, or the first 128 bits of data if the BlackBerry Desktop Software supports Triple DES encryption
8. deletes any bits of data that it does not use to generate the device transport key

Message keys

A BlackBerry Enterprise Server and BlackBerry device generate one or more message keys that are designed to protect the integrity of the data (for example, short keys or large messages) that the BlackBerry Enterprise Server and device send between each other. If a message exceeds 2 KB and consists of several data packets, the BlackBerry Enterprise Server and device generate a unique message key for each data packet.

Each message key consists of random data that is designed to make it difficult for a third party to decrypt, re-create, or duplicate the message key.

The BlackBerry Enterprise Server and device do not store the message keys but they free the memory that is associated with the message keys after the BlackBerry Enterprise Server or device uses the message keys to decrypt the message.

Data flow: Generating a message key on a BlackBerry Enterprise Server

A BlackBerry Enterprise Server is designed to use the DSA PRNG function to generate a message key.

To generate a message key, the BlackBerry Enterprise Server performs the following actions:

1. retrieves random data from multiple sources for the seed, using a technique that the BlackBerry Enterprise Server derives from the initialization function of the ARC4 encryption algorithm
2. uses the random data to reorder the contents of a 256-byte state array (also known as a 2048-bit state array)

   If the Microsoft Cryptographic API exists on the computer that hosts the BlackBerry Enterprise Server, the BlackBerry Enterprise Server requests 512 bits of randomness from the Microsoft Cryptographic API to increase the randomness of the data.
3. adds the 256-byte state array into the ARC4 algorithm to further randomize the 256-byte state array
4. draws 521 bytes from the 256-byte state array

   The BlackBerry Enterprise Server draws an additional 9 bytes for the 256-byte state array, for a total of 521 bits (512 + 9 = 521) to make sure that the pointers before and after the generation process are not in the same place, and in case the first few bytes of the 256-byte state array are not random.
5. uses SHA-512 to hash the 521-byte value to 64 bytes
6. uses the 64-byte value to seed the DSA PRNG function

   The BlackBerry Enterprise Server stores a copy of the seed in a file. When the BlackBerry Enterprise Server restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.
7. uses the DSA PRNG function to generate 256 pseudorandom bits for use with AES encryption and 128 pseudorandom bits for use with Triple DES encryption
8. uses the pseudorandom bits with AES encryption or Triple DES encryption to generate the message key

For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*.

Data flow: Generating a message key on a device

A BlackBerry device uses the DRBG function if the device is operating in FIPS mode, and the DSA PRNG function if the device is not operating in FIPS mode, to generate a message key.

To generate a message key, the device performs the following actions:

1. Retrieves random data from multiple sources to generate the seed using a technique that the device derives from the initialization function of the ARC4 encryption algorithm
2. Uses the random data to reorder the contents of a 256-byte state array (also known as a 2048-bit state array)
3. Adds the 256-byte state array into the ARC4 encryption algorithm to further randomize the 256-byte state array
4. Draws 521 bytes from the ARC4 state array

   The device draws an additional 9 bytes for the 256-byte state array, for a total of 521 bytes (512 + 9 = 521) to make sure that the pointers before and after the call are not in the same place, and in case the first few bytes of the ARC4 state array are not random
5. Uses SHA-512 to hash the 521-byte value to 64 bytes
6. Uses the 64-byte value to seed the DRBG function (if the device is not operating in FIPS mode, the device uses the DSA PRNG function)

   The device stores a copy of the seed in a file. When the device restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.
7. Uses the DRBG function to generate 128 pseudorandom bits for use with Triple DES encryption and 256 pseudorandom bits for use with AES encryption (if the device is not operating in FIPS mode, the device uses the DSA PRNG function)
8. Uses the pseudorandom bits to create the message key

For more information about the DRBG function, see *NIST Special Publication 800-90*. For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*.

Content protection keys

When you or a user turns on content protection for a BlackBerry device, the BlackBerry device generates a content protection key. The content protection key is designed to encrypt user data on the BlackBerry device when it is locked.

When the BlackBerry device is locked, an encryption process begins. The BlackBerry device frees the memory that it associates with the content protection key and ECC private key that it stores in RAM. The BlackBerry device then uses the ECC public key to encrypt new data that it receives.

When a user unlocks a BlackBerry device, the BlackBerry device decrypts the content protection key and ECC private key in flash memory. When the user wants to view data, the BlackBerry device uses the content protection key or ECC private key to decrypt the data before the BlackBerry device displays it. An unlocked BlackBerry device uses the content protection key to encrypt new data that the user types or adds to the BlackBerry device, or that the BlackBerry device receives.

Data flow: Turning on content protection using a BlackBerry Enterprise Server

You can turn on content protection using a BlackBerry Enterprise Server when you configure the Content Protection Strength IT policy rule.

1. The BlackBerry Enterprise Server performs the following actions:
   a selects *b* randomly
   b calculates $B = bP$
   c stores *b* in the BlackBerry Configuration Database
   d sends *B* in the IT policy to the BlackBerry device
2. The device performs the following actions:
   a verifies that *B* is a valid public key
   b selects *d* randomly
   c calculates $D = dP$
   d stores *D* in flash memory
   e calculates $K = dB$
   f uses *K* to encrypt the current device password
   g uses the encrypted device password to encrypt the content protection key
   h permanently deletes *d* and *K*

When the device permanently deletes *d*, the device is designed so that a potentially malicious user cannot use the data that remains on the device to recover *K*. Only the BlackBerry Enterprise Server knows *b* and can recalculate $K = dB = dbP = bD$ if the BlackBerry Enterprise Server is provided with *D*. The BlackBerry Enterprise Solution uses K when it resets the device password when content protection is turned on.

Data flow: Generating a content protection key on a device

When you or a BlackBerry device user turns on content protection on the device for the first time, the device performs the following actions:

1. Uses a DRBG function to generate a content protection key (if the device is not operating in FIPS mode, the device uses a DSA PRNG function)
2. Generates an ECC key pair with a bit length that you or the user determines

3. Prompts the user to type the device password
4. Derives an ephemeral 256-bit AES encryption key from the device password, using PKCS #5
5. Uses the ephemeral key to encrypt the content protection key and ECC private key
6. Stores the encrypted content protection key, encrypted ECC private key, and ECC public key in flash memory

The content protection key is a semi-permanent 256-bit AES encryption key. If the user changes the device password, the device uses the new password to derive a new ephemeral key. The device uses the new ephemeral key to re-encrypt the versions of the content protection key and ECC private key that are in flash memory.

For more information about the DRBG function, see *NIST Special Publication 800-90*. For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*. For more information about PKCS #5, visit www.rsa.com to see *PKCS #5: Password-Based Cryptography Standard*.

Data flow: Deriving an ephemeral key that protects a content protection key and ECC private key

A BlackBerry device uses an ephemeral key to encrypt a content protection key and ECC private key. The device derives the ephemeral key, which is an AES-256 encryption key, from the device password using PKCS #5.

To derive an ephemeral key, the device performs the following actions:

1. selects a 64-bit salt (which is random data that the BlackBerry device mixes with the device password)

   The salt prevents two identical passwords from turning into the same key.
2. concatenates the salt, password, and salt again into a byte array (for example, `Salt|Password|Salt`)
3. hashes the byte array with SHA-256
4. stores the resulting hash in a byte array that is called a key

```
(key) =
SHA256(Salt|Password|Salt)
```

5. hashes the key 18 more times and stores the result in the key each time

   For example, for i=0 to 18, the device performs the following actions:

```
(key) = SHA256(key)
 i++
 done
```

The final hash creates the ephemeral key.

For more information, visit www.rsa.com to see *PKCS #5: Password-Based Cryptography Standard*.

Principal encryption keys

When you or a user turns on content protection for device transport keys, a BlackBerry device generates a principal encryption key and stores it in flash memory. The device uses the principal encryption key to encrypt the device transport keys that are stored on the device in flash memory and the PIN encryption key that is specific to your organization. The device encrypts the principal encryption key using the content protection key. When the device receives data that the device transport key encrypts while the device is locked, the device uses the principal encryption key to decrypt the device transport key that is in flash memory.

Data flow: Generating a principal encryption key

When you or a user turns on content protection for device transport keys on a BlackBerry device for the first time, the device performs the following actions:

1. generates a principal encryption key, which is an AES-256 encryption key
2. stores the decrypted principal encryption key in RAM
3. uses the existing content protection key to encrypt the principal encryption key
4. stores the encrypted principal encryption key in flash memory

When the device locks, the device uses the decrypted principal encryption key to encrypt the device transport keys that are stored in the flash memory of the device.

PIN encryption keys

The PIN encryption key is a Triple DES 168-bit key that a BlackBerry device uses to encrypt PIN messages that it sends to other devices and to authenticate and decrypt PIN messages that it receives from other devices. If a BlackBerry device user knows the PIN of another device, the user can send a PIN message to the device. Unlike an email message that a user sends to an email address, a PIN message bypasses the BlackBerry Enterprise Server and your organization's network.

By default, each device uses the same global PIN encryption key, which Research In Motion adds to the device during the manufacturing process. The global PIN encryption key permits every device to authenticate and decrypt every PIN message that the device receives. Because all devices share the same global PIN encryption key, there is a limit to how effectively PIN messages are encrypted. PIN messages are not considered as confidential as email messages that are sent from the BlackBerry Enterprise Server, which use BlackBerry transport layer encryption. Encryption using the global PIN encryption key is sometimes referred to as "scrambling".

If the security policies of your organization require additional confidentiality for PIN messages, you can generate a PIN encryption key that is specific to your organization or configure S/MIME encryption or PGP encryption for PIN messages.

A device that has a PIN encryption key that is specific to your organization can perform the following actions:

- can only encrypt PIN messages sent to other devices on your organization's network that use the same PIN encryption key
- can only decrypt PIN messages that are sent from devices that use the global PIN encryption key or PIN messages from other devices on your organization's network that use the same PIN encryption key
- cannot decrypt PIN messages sent from devices that use a PIN encryption key from another organization

You can generate a PIN encryption key for your organization and send it to devices using the BlackBerry Administration Service.

When you use a PIN encryption key that is specific to your organization, BlackBerry Messenger messages also use the PIN encryption key. If you use a PIN encryption key that is specific to your organization, you limit users so that they can only use BlackBerry Messenger with other users in your organization and you create a closed community within your organization.

Optionally, you can configure the Firewall Block Incoming Messages IT policy rule to block PIN messages that are sent from devices that have the global PIN encryption key. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide.*

4 Encrypting data that the BlackBerry Enterprise Server and a device send to each other

To encrypt data that is in transit between the BlackBerry Enterprise Server and a BlackBerry device in your organization, the BlackBerry Enterprise Solution uses BlackBerry transport layer encryption. BlackBerry transport layer encryption is designed to encrypt data from the time that a device user sends a message from the device to when the BlackBerry Enterprise Server receives the message, and from the time that the BlackBerry Enterprise Server sends a message to when the device receives the message.

Before the device sends a message, it compresses and encrypts the message using the device transport key. When the BlackBerry Enterprise Server receives a message from the device, the BlackBerry Dispatcher decrypts the message using the device transport key, and then decompresses the message.

Algorithms that the BlackBerry Enterprise Solution uses to encrypt data

The BlackBerry Enterprise Solution uses AES or Triple DES as the symmetric key cryptographic algorithm for encrypting data. By default, the BlackBerry Enterprise Server uses the strongest algorithm that both the BlackBerry Enterprise Server and the BlackBerry device support for BlackBerry transport layer encryption.

If you configure the BlackBerry Enterprise Server to support AES and Triple DES, by default, the BlackBerry Enterprise Solution generates device transport keys using AES encryption. If a device uses BlackBerry Device Software version 3.7 or earlier or BlackBerry Desktop Software version 3.7 or earlier, the BlackBerry Enterprise Solution generates the device transport keys of the device using Triple DES.

How the BlackBerry Enterprise Solution uses AES to encrypt data

By default, when a BlackBerry device supports AES, the BlackBerry Enterprise Solution uses AES for BlackBerry transport layer encryption. The BlackBerry Enterprise Solution uses AES in CBC mode to generate the message keys and device transport keys. The keys consist of 256 bits of data.

BlackBerry Enterprise Server version 4.0 or later, BlackBerry Device Software version 4.0 or later, and BlackBerry Desktop Software version 4.0 or later support AES.

For more information about how the BlackBerry Enterprise Server uses AES for BlackBerry transport layer encryption to communicate with devices, visit www.blackberry.com/support to read article KB05429.

How a device uses the AES algorithm to help protect user data and keys

The BlackBerry device implementation of the AES algorithm is designed to help protect user data and keys (such as the device transport key and ephemeral key) from traditional attacks and side-channel attacks.

A traditional attack tries to exploit data that a cryptographic system stores or transmits. The potentially malicious user tries to determine the key or the plain-text data by exploiting a weakness in the design of the cryptographic algorithm or protocol.

The potentially malicious user uses a side-channel attack to try to exploit the physical properties of the device implementation of the AES algorithm using power analysis (for example, SPA and DPA) and electromagnetic analysis (for example, SEMA and DEMA). A potentially malicious user tries to determine the keys that the device uses by measuring and analyzing the power consumption or the electromagnetic radiation that the device emits during cryptographic operations. The device uses a masking operation, table splitting, and a random mask application to help protect the keys and plain-text data against side-channel attacks at all points during the encryption and decryption operations.

Data flow: Running a masking operation during the first AES calculation when content protection is turned on

During the first AES calculation, the BlackBerry device performs the following actions if you or a user turned on content protection:

1. runs a masking operation by performing the following actions:
   a. creates a mask table (*M*), where each table entry is a random value
   b. creates a masked version of the S-Box table (*S'*) that is used within AES
   c. periodically and randomly changes the order of all table entries
2. runs the result of step 1 as the input through both *M* and *S'*
3. combines the output of step 2 from *M* and *S'*
4. deletes the mask and produces the AES output

Data flow: Running a masking operation during subsequent AES calculations when content protection is turned on

A BlackBerry device performs the following actions:

1. performs the masking operation by periodically and randomly permuting all table entries in every calculation
2. runs the input through both *M* and *S'*
3. combines the output from *M* and *S'*
4. deletes the mask and produces the AES output

Data flow: Running a masking operation when a device does not use content protection

If you or a user did not turn on content protection, a BlackBerry device performs the following actions during an AES calculation:

1. masks the output from the round key
2. masks the AES S-Box input
3. masks the AES S-Box output

How the AES algorithm creates S-Box tables and uses round keys and masks

A BlackBerry device permutes each AES S-Box entry at random and masks each entry with a random value.

The BlackBerry device masks the round keys with random values and any S-Box masks that the AES algorithm requires to work. Round keys are subkeys that the key schedule calculates for each round of encryption.

The BlackBerry device changes the random masks periodically and uses extra S-Box data to make identification of the S-Box table difficult, whether the BlackBerry device uses the S-Box table in the encryption process, decryption process, or key schedule process.

How the BlackBerry Enterprise Solution uses Triple DES to encrypt data

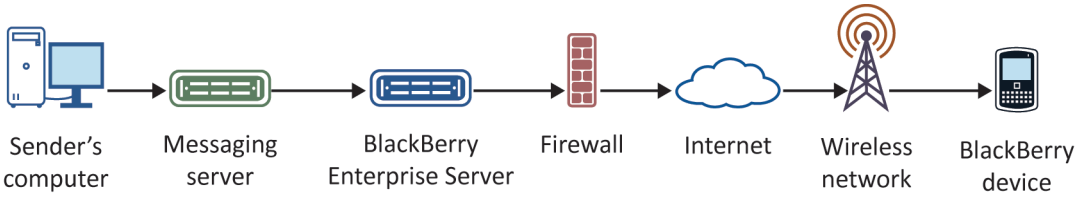
The BlackBerry Enterprise Solution uses a two-key Triple DES encryption algorithm to generate message keys and device transport keys. In the three iterations of the DES algorithm, the first 56-bit key in outer CBC mode encrypts the data, the second 56-bit key decrypts the data, and the first key encrypts the data again.

The BlackBerry Enterprise Solution stores the message keys and device transport keys as 128-bit binary strings with each parity bit in the least significant bit of each of the 8 bytes of key data. The message keys and device transport keys have overall key lengths of 112 bits and include 16 bits of parity data.

All versions of the BlackBerry Enterprise Server, BlackBerry Device Software, and BlackBerry Desktop Software support Triple DES.

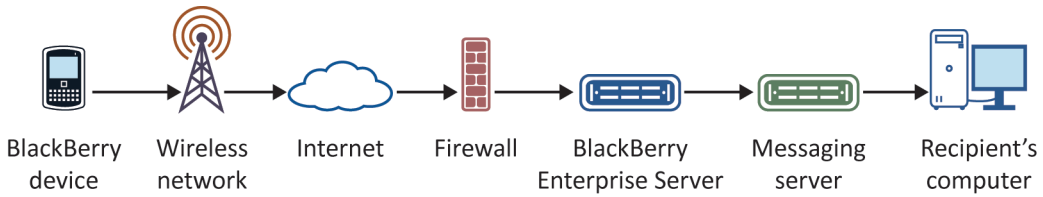
For more information about Triple DES, see *Federal Information Processing Standard - FIPS PUB 81 [3]*.

Data flow: Sending an email message to a device using BlackBerry transport layer encryption



1. A sender sends an email message to a BlackBerry device user.
2. The BlackBerry Enterprise Server performs the following actions:
   a compresses the email message
   b encrypts the email message using the message key
   c encrypts the message key using the device transport key of the device
   d sends the encrypted email message and encrypted message key to the device
3. The BlackBerry device user clicks on the email message on the device to open it.
4. The device performs the following actions:
   a decrypts the message key using the device transport key
   b decrypts the email message using the message key
   c decompresses the email message
   d displays the email message to the user

Data flow: Sending an email message from a device using BlackBerry transport layer encryption



1. A sender sends an email message from a BlackBerry device to a recipient.
2. The device performs the following actions:
   a compresses the email message
   b encrypts the compressed email message using the message key
   c encrypts the message key using the device transport key of the device
   d sends the encrypted message key and encrypted email message to the BlackBerry Enterprise Server
3. The BlackBerry Enterprise Server performs the following actions:
   a decrypts the message key using the device transport key
   b decrypts the email message using the message key
   c decompresses the email message
   d forwards the email message to the recipient

Managing BlackBerry Enterprise Solution security

5

Using an IT policy to manage BlackBerry Enterprise Solution security

You can use an IT policy to control and manage BlackBerry devices, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager in your organization's environment. An IT policy consists of multiple IT policy rules that manage the security and behavior of the BlackBerry Enterprise Solution. For example, you can use IT policy rules to manage the following security features and behaviors of the device:

- encryption (for example, encryption of user data and messages that the BlackBerry Enterprise Server forwards to message recipients) and encryption strength
- use of a password or pass phrase
- connections that use Bluetooth wireless technology
- protection of user data and device transport keys on the device
- control of device resources, such as the camera or GPS, that are available to third-party applications

The BlackBerry Enterprise Server includes preconfigured IT policies that you can use to manage the security of the BlackBerry Enterprise Solution. The Default IT policy includes IT policy rules that are configured to indicate the default behavior of the device or BlackBerry Desktop Software.

After a device user activates a device, the BlackBerry Enterprise Server automatically sends to the device the IT policy that you assigned to the user account or group. By default, if you do not assign an IT policy to the user account or group, the BlackBerry Enterprise Server sends the Default IT policy. If you delete an IT policy that you assigned to the user account or group, the BlackBerry Enterprise Server automatically re-assigns the Default IT policy to the user account and resends the Default IT policy to the device.

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide.*

Preconfigured IT policies

The BlackBerry Enterprise Server includes the following preconfigured IT policies that you can change to create IT policies that meet the requirements of your organization.

Preconfigured IT policy	Description
Default	This policy includes all the standard IT policy rules that are set on the BlackBerry Enterprise Server.
Individual-Liable Devices	Similar to the Default IT policy, this policy prevents BlackBerry device users from accessing organizer data from within the social networking applications on their BlackBerry devices. This policy permits users to access their personal calendar services and email messaging services (for example, their BlackBerry Internet Service accounts), update the BlackBerry Device Software using methods that exist outside your organization, make calls when devices are locked, and cut, copy, and paste text. Users cannot forward email messages from one email messaging service to another. You can use the Individual-Liable Devices IT policy if your organization includes users who purchase their own devices and connect the devices to a BlackBerry Enterprise Server instance in your organization's environment.
Basic Password Security	Similar to the Default IT policy, this policy also requires a basic password that users can use to unlock their devices. Users must change the passwords regularly. The IT policy includes a password timeout that locks devices.
Medium Password Security	Similar to the Default IT policy, this policy also requires a complex password that users can use to unlock their devices. Users must change the passwords regularly. This policy includes a maximum password history and turns off Bluetooth technology on devices.
Medium Security with No 3rd Party Applications	Similar to the Medium Password Security, this policy requires a complex password that a user must change frequently, a security timeout, and a maximum password history. This policy prevents users from making their devices discoverable by other Bluetooth enabled devices and prevents devices from downloading third-party applications.
Advanced Security	Similar to the Default IT policy, this IT policy also requires a complex password that users must change frequently, a password timeout that locks devices, and a maximum password history. This policy restricts Bluetooth technology on devices, turns on strong content protection, turns off USB mass storage, and requires devices to encrypt external file systems.
Advanced Security with No 3rd Party Applications	Similar to the Advanced Security IT policy, this IT policy requires a complex password that users must change frequently, a password timeout that locks devices, and a maximum password history. This policy restricts Bluetooth technology on devices, turns on strong content protection, turns off USB mass storage, requires devices to encrypt external file systems, and prevents devices from downloading third-party applications.

Using IT policy rules to manage BlackBerry Enterprise Solution security

You can use IT policy rules to customize and control the actions that the BlackBerry Enterprise Solution can perform.

To use an IT policy rule on a BlackBerry device, you must verify that the BlackBerry Device Software version supports the IT policy rule. For example, you cannot use the Disable Camera IT policy rule to control whether a BlackBerry device user can access the camera on the device if the BlackBerry Device Software version does not support the IT policy rule. For information about the BlackBerry Device Software version that is required for a specific IT policy rule, see the *BlackBerry Enterprise Server Policy Reference Guide*.

If you create a custom IT policy that does not permit users to change their user information on their devices, you can only apply this custom IT policy to devices running BlackBerry Device Software 5.0 or later.

The BlackBerry Administration Service groups the IT policy rules by common properties or by application. Most IT policy rules are designed so that you can assign them to multiple user accounts and groups.

Sending an IT policy over the wireless network

If your organization's environment includes C++ based BlackBerry devices that are running BlackBerry Device Software version 2.5 or later or Java based devices that are running BlackBerry Device Software version 3.6 or later, the BlackBerry Enterprise Server can send changes to IT policies to a device over the wireless network automatically. When the device receives an updated IT policy or a new IT policy, the device, BlackBerry Desktop Software, and BlackBerry Web Desktop Manager apply the configuration changes immediately.

By default, the BlackBerry Enterprise Server is designed to resend an IT policy to the device within a short period of time after you update the IT policy using the BlackBerry Administration Service. You can also resend an IT policy to a specific device manually. You can configure the BlackBerry Enterprise Server to resend the IT policy to the device at scheduled intervals regardless of whether you changed the IT policy.

Assigning IT policies and resolving IT policy conflicts

You can assign IT policies directly to a user account or to a group. By default, if you do not assign an IT policy to a user account or a group that the user is a member of, the BlackBerry Enterprise Server applies the Default IT policy to the user account. If you assign an IT policy to a group that a user account is a member of, the BlackBerry Enterprise Server applies the group IT policy to the user account. If you assign an IT policy to the user account directly, the BlackBerry Enterprise Server applies this IT policy to the user account instead of the group IT policy or Default IT policy.

If a user account is a member of multiple groups that have different IT policies, the BlackBerry Enterprise Server must determine which IT policy to apply to the user account. You must use one of the following reconciliation options:

Method	Description
Apply one IT policy to the user account	The BlackBerry Enterprise Server applies one of the group IT policies to the user account. You specify rankings for the available IT policies using the BlackBerry Administration Service and the BlackBerry Enterprise Server applies the IT policy with the highest ranking. If you upgrade to BlackBerry Enterprise Server 5.0 SP2 or later from a previous version of the BlackBerry Enterprise Server, this is the default method for resolving IT policy conflicts.
Apply multiple IT policies to the user account	The BlackBerry Enterprise Server applies all of the group IT policies to the user account, resulting in a combined IT policy that has a unique ID. The BlackBerry Enterprise Server resolves conflicting IT policy rules using the ranking of the available IT policies that you specified using the BlackBerry Administration Service. If an IT policy rule is different in the multiple IT policies, the BlackBerry Enterprise Server applies the rule setting from the IT policy that you ranked the highest. If you install BlackBerry Enterprise Server 5.0 SP2 or later, this is the default method for resolving IT policy conflicts.

Reconciliation rules for conflicting IT policies when you apply one IT policy to the user account

The BlackBerry Enterprise Server can apply only one IT policy to a user account. Since you can assign IT policies to user accounts, groups, or the BlackBerry Domain, the BlackBerry Administration Service uses predefined rules to determine which IT policy it can apply to a user account.

The BlackBerry Administration Service might have to reconcile conflicting IT policies if you perform any of the following actions:

- add an IT policy to or remove an IT policy from a user account or group
- change an IT policy
- change the ranking of IT policies
- delete an IT policy

Scenario	Rule
You add a new user account to a BlackBerry Enterprise Server. You do not assign an IT policy directly to the user account and you do not add the user to a group.	The IT policy that you assigned to the BlackBerry Domain, or the Default IT policy that is assigned to the BlackBerry Domain, is assigned to the user account.
You assign an IT policy to a user account and a different IT policy to a group that the user account belongs to.	The IT policy that you assign to a user account takes precedence over an IT policy that you assign to a group. An IT policy that you assign to a group takes precedence over the IT policy that you assign to the BlackBerry Domain (or the Default IT policy).

Scenario	Rule
A user account belongs to multiple groups. You assign multiple IT policies to the groups but do not assign an IT policy to the user account.	The BlackBerry Enterprise Server applies the IT policy that you ranked the highest in the BlackBerry Administration Service to the user account.

Reconciliation rules for conflicting IT policies when you apply multiple IT policies to a user account

The BlackBerry Enterprise Server can apply multiple IT policies to a user account if the user account is a member of multiple groups that have different IT policies. Since you can assign IT policies to user accounts, groups, or the BlackBerry Domain, the BlackBerry Administration Service uses predefined rules to apply an IT policy to a user account.

The BlackBerry Administration Service might have to reconcile conflicting IT policies if you perform any of the following actions:

- add an IT policy to or remove an IT policy from a user account or group
- change an IT policy
- change the ranking of IT policies
- delete an IT policy

Scenario	Rule
You add a new user account to a BlackBerry Enterprise Server. You do not assign an IT policy directly to the user account and you do not add the user account to a group.	The Default IT policy (applied at the BlackBerry Domain level) is assigned to the user account.
You assign an IT policy to a user account and different IT policies to the groups that the user account belongs to.	The IT policy that you assign to a user account takes precedence over the IT policies that you assign to the groups that the user belongs to. An IT policy that you assign to a group takes precedence over the Default IT policy (applied at the BlackBerry Domain level).
A user account belongs to multiple groups. You assign multiple IT policies to the groups but you do not assign an IT policy to the user account.	If you assign multiple IT policies to the groups that the user account belongs to, the BlackBerry Enterprise Server resolves the IT policy rule settings in the multiple IT policies and assigns a combined IT policy that has a unique ID to the user account. The BlackBerry Enterprise Server resolves conflicting settings for IT policy rules by applying the rule setting from the IT policy that you ranked the highest in the BlackBerry Administration Service. For example, you configure the Disable Photo Camera IT policy rule to Yes in IT policy A and to No in IT policy B. If you rank IT policy A higher than IT policy B, the Yes setting is applied for this rule.
A user account belongs to two groups. You assign the first group IT policy A, which has the Allow Browser IT policy	When the BlackBerry Enterprise Server resolves conflicting rule settings, any rule settings that have been explicitly configured to a value take precedence over IT policy rule settings that are blank (these rules revert to the default value).

Scenario	Rule
rule as blank (which means that it uses the default value of Yes). You assign the second group IT policy B, which has the Allow Browser IT policy rule set to No. You ranked IT policy A higher than IT policy B in the BlackBerry Administration Service.	For example, in this scenario, the Allow Browser IT policy rule setting from IT policy B, No, is applied to the user account even though IT policy A is ranked higher than IT policy B, because the Allow Browser IT policy rule is blank in IT policy A. If the Allow Browser IT policy rule was configured to Yes in IT policy A, the Yes value would be applied to the user account.

Best practice: Controlling which applications can use the GPS feature on a device

By default, if a third-party application or a preloaded BlackBerry Application on a BlackBerry device supports the GPS feature, the application can use the GPS feature. For example, BlackBerry Maps is a preloaded BlackBerry Application that uses the GPS feature to permit a user to locate a global position.

Best practice	Description
Control which application on the device can use the GPS feature.	Consider preventing a third-party application or preloaded BlackBerry Application from accessing the global position of the device. To apply this best practice, you can use one of the following methods: • To prevent the device from permitting all third-party applications and preloaded BlackBerry Applications from accessing the GPS feature, change the value of the Disable GPS IT policy rule to Yes. • To prevent a third-party application from using the GPS feature, change the value of the Is Access to the GPS API Allowed application control policy rule to Not Permitted. Assign the application control policy to the software configuration.
Control when the device reports its location to the BlackBerry Enterprise Server.	By default, the device does not use the GPS feature to report its location to the BlackBerry Enterprise Server. If you change the value for the Enable Enterprise Location Tracking IT policy rule to Yes, consider configuring the interval after which a device reports its location to the BlackBerry Enterprise Server. To apply this best practice, you can use the Enterprise Location Tracking Interval IT policy rule. You can also use the Enterprise Location Tracking User Prompt Message IT policy rule to create a message that the device displays to

Best practice	Description
	notify the user that you turned on the ability of the device to report its location to the BlackBerry Enterprise Server.

Using IT administration commands to protect a lost or stolen device

The BlackBerry Enterprise Server includes IT administration commands that you can send over the wireless network to protect sensitive data on a BlackBerry device. You can use the commands to lock the device, permanently delete work data, permanently delete user information and application data, and return the device settings to the default values.

IT administration command	Description
Specify new device password and lock device	This command creates a new password and locks a device over the wireless network. You can communicate the new password to the user verbally when the BlackBerry device user locates the device. When the user unlocks the device, the device prompts the user to accept or reject the new password. You can use this command if the device is lost. If you or a user turned on content protection and a device is running BlackBerry Device Software 4.3.0 or later, you can use this command. If you or a user turned on two-factor content protection, you cannot use this command.
Delete only the organization data and remove device	This command permanently deletes all work data that the device stores and removes the device from the BlackBerry Enterprise Server. All personal data remains on the device. You can send this command to a personal device when a user no longer works at your organization and you want to delete work data from the device. You can also specify whether you want to delete or disable a user account from the BlackBerry Enterprise Server after the device deletes all work data.
Delete all device data and remove device	This command permanently deletes all user information and application data that the device stores. You can configure the following options when you use this command: • specify a delay, in hours, that must occur before the device starts to delete all the user information and application data • require the device to return to its factory default settings when it receives this command • specify whether to permit the user to stop permanently deleting data from the device and making the device unavailable during the delay period

IT administration command	Description
	You can send this command to a device that you want to distribute to another user in your organization, or to a device that is lost and that the user might not recover. You can also specify whether you want to delete or disable a user account from the BlackBerry Enterprise Server after the device deletes all user information and application data.

Data flow: Sending the Specify new device password and lock device IT administration command when content protection is turned on

1. The BlackBerry Enterprise Server sends the Specify new device password and lock device IT administration command and the new BlackBerry device password to the device.
2. The device performs the following actions:
   a selects r randomly
   b stores r in RAM
   c calculates $D' = rD = rdP$
   d calculates $h = SHA\text{-}1(B)$
   e sends D' and h to the BlackBerry Enterprise Server
3. The BlackBerry Enterprise Server performs the following actions:
   a uses h to determine which B the device used and which b to use
   b verifies that D' is a valid public key
   c calculates $K' = bD' = brdP = rdB = rK$ (the BlackBerry Enterprise Server knows only rK and cannot calculate K without r)
   d calculates $h = \text{SHA-1}(D')$
   e sends the new device password, K', and h to the device
4. The device performs the following actions:
   a uses h to verify that K' is associated with D' and r
   b verifies that K' is a valid public key
   c calculates $r^{-1}K' = r^{-1}rK = K$
   d permanently deletes r
   e uses K to decrypt the content protection key

f permanently deletes *K*

5. The device performs the following actions:
   a selects *d* randomly
   b calculates *D* = *dP*
   c stores *D* in flash memory
   d calculates *K* = *dB*
   e uses *K* to encrypt the new BlackBerry device password
   f uses the encrypted new password to encrypt the content protection key

Managing device access to the BlackBerry Enterprise Server

You can use the Enterprise Service Policy to control which BlackBerry devices can connect to a BlackBerry Enterprise Server. By default, after you turn on the Enterprise Service Policy, the BlackBerry Enterprise Server permits connections from any device that you previously associated with the BlackBerry Enterprise Server. The BlackBerry Enterprise Server also prevents connections from any device that you associate with the BlackBerry Enterprise Server after you turn on the Enterprise Service Policy.

You can configure an allowed list to determine which devices can access a BlackBerry Enterprise Server. A device that meets the criteria that you specify in the allowed list can associate with the BlackBerry Enterprise Server when the device activates over the wireless network.

You can define the following types of criteria:

- specific device PINs
- range of device PINs
- specific manufacturers
- specific device models

The BlackBerry Administration Service includes lists of permitted manufacturers and models of devices that you associated with the BlackBerry Enterprise Server previously.

You can permit a user to override the Enterprise Service Policy so that a device can connect to the BlackBerry Enterprise Server even if you configure the allowed list with criteria that exclude that device.

For more information, see the *BlackBerry Enterprise Server Administration Guide*.

Using a segmented network to help prevent the spread of malware

To help prevent the spread of malware in your organization's network, you can use firewalls to divide your organization's network or LAN into segments to create a segmented network. Each segment can manage the network traffic for a specific BlackBerry Enterprise Server component. A segmented network is designed to improve the security and performance of the segments by filtering out data that is not sent to the correct segment.

To configure the BlackBerry Enterprise Server in a segmented network, you must install each BlackBerry Enterprise Server component on a computer that is separate from the computers that host other components and then place each computer in its own network segment. If you configure the BlackBerry Enterprise Server in a segmented network, you create an architecture that is designed to prevent the spread of potential attacks from one computer that hosts a component to another computer within your organization's LAN. A segmented network architecture is designed to isolate attacks and contain them on one computer. To permit communication with other components, when you install each component in its own segment, you open only the port numbers that the components use.

The BlackBerry Enterprise Server and components, with the exception of the BlackBerry Router, do not support installation in a DMZ. For more information about configuring the BlackBerry Router in the DMZ, visit www.blackberry.com/go/serverdocs to see *Placing the BlackBerry Router in the DMZ*.

For more information about the port numbers that the components use, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Enterprise Server Administration Guide*.

Moving a device to a BlackBerry Enterprise Server that uses a different BlackBerry Configuration Database

If you move a BlackBerry device to a BlackBerry Enterprise Server that uses a different BlackBerry Configuration Database without using the BlackBerry Enterprise Transporter, you or a user must permanently delete all user data and application data, the device transport key, and the IT policy public key from the device.

You or the user must reactivate the device to generate a new device transport key. The BlackBerry Enterprise Server that you move the device to must generate an IT policy key pair and digitally sign and send the IT policy and the IT policy public key to the device before the device can communicate with the BlackBerry Enterprise Server.

The BlackBerry Configuration Database that you migrated the device to stores the BlackBerry Enterprise Server name, the device transport key, and the IT policy private key.

Configuring the IT Policy Viewer icon on a device

The IT policy viewer permits a BlackBerry device user to view IT policy rules that were configured for a BlackBerry device that is running BlackBerry Device Software 6.0 or later. Only devices that you activate on a BlackBerry Enterprise Server include the IT policy viewer.

The IT policy viewer can display IT policy rules from the following policy groups:

- Camera policy group
- Password policy group
- Security policy group (except for the Forbidden Passwords IT policy rule and Duress Notification Address IT policy rule)

The IT policy viewer can also display the following IT policy rules:

- Disable Voice Note Recording IT policy rule
- Password Required IT policy rule
- Minimum Password Length IT policy rule
- Maximum Password Age IT policy rule
- Password Pattern Checks IT policy rule
- Disable Bluetooth IT policy rule

To open the IT policy viewer, in the Security options on the device, a user can click View IT Policy. A user can also change the device options so that the IT Policy Viewer icon appears in a folder that the user chooses on the device. To require that the IT Policy Viewer Icon appears in a folder on the device, you can use the Force Display IT Policy Viewer Icon on Homescreen IT policy rule.

Device storage space

6

The BlackBerry device storage space consists of various sections that store BlackBerry device user data and sensitive information such as encryption keys. Third-party applications on a device cannot write to or access the sections that store sensitive information.

The following sections are a part of the device storage space.

Section	Description
application storage	The application storage is an internal file system on a device that stores application data and user data. Application storage is the only place on a device from which applications can be run. Sections of application storage can store files that a user downloads or saves to device memory. You cannot remove the application storage from the device. The application storage is encrypted when content protection is turned on.
built-in media storage	The built-in media storage stores files that a user saves on a device. The device uses and exposes the built-in media storage the same way that the device uses and exposes a media card. When you permanently delete or a user permanently deletes all device data, the device deletes all files from the built-in media storage, except for the file system partition called System, which includes sample pictures and sample ring tones. The built-in media storage is encrypted when content protection is turned on.
NV store	The NV store persists in application storage, and only the operating system of the device can write to it. Third-party application code cannot write to the NV store.
media card	The media card is a microSD card that a device user inserts in the device to extend the amount of storage on the device. A user can save, access, and encrypt files on the media card using the device. When you permanently delete or a user permanently deletes device data, the device deletes the files from the media card only if the device is running BlackBerry Device Software 5.0 or later and if you configure the Media Card Format on Device Wipe IT policy rule.

Changing when a device cleans the device memory

By default, the memory cleaner application runs on a BlackBerry device when the device is inactive for a specified period of time. You or a BlackBerry device user can change when the memory cleaner application runs when any the following conditions exist:

- The user synchronizes the device with a computer.
- The user locks the device.
- The device locks after it is inactive for a specified period of time.
- The user changes the time or time zone on the device.

To change when the memory cleaner application runs, you can use IT policies or the user can turn on or turn off the memory cleaner application in the Security options on the device.

You or the user cannot turn off the memory cleaner application on the device if any of the following conditions exist:

- You or the user turns on content protection on the device.
- An application uses the RIM Cryptographic API to create a private key or symmetric key.
- An application that registers with the memory cleaner application requires that memory cleaning application be turned on.
- The device user installs the S/MIME Support Package for BlackBerry smartphones on the device and a private key exists on the device.
- The user installs the PGP Support Package for BlackBerry smartphones on the device and a private key exists on the device.

If you or the user turns on the memory cleaner application, based garbage collection process uses the memory cleaner application automatically. The garbage collection process overwrites data that the device no longer uses.

For more information about the IT policy rules that you can use to change when the memory cleaner application runs, see the *BlackBerry Enterprise Server Policy Reference Guide*.

When a device overwrites data in the device memory

A BlackBerry device continually runs the memory cleaner application during the based garbage collection process to overwrite data in the device memory that the device no longer uses.

The device runs the garbage collection process when any of the following conditions exist:

- You or a device user turns on content protection for the device.
- An application uses the RIM Cryptographic API to create a private key or symmetric key.
- A third-party application turns on the garbage collection process by registering with the memory cleaner application on the device. The memory cleaner application instructs applications to empty caches and to free the device memory that is associated with sensitive application data that the applications no longer use.
- A BlackBerry device user installs the S/MIME Support Package for BlackBerry smartphones on the device.
- A device user installs the PGP Support Package for BlackBerry smartphones on the device.

When the device runs the garbage collection process, the garbage collection process overwrites the data that the device no longer uses with zeroes, periodically runs the memory cleaner application, and overwrites the memory that the memory cleaner application frees.

Deleting all device data from the device storage space

A BlackBerry device is designed to permanently delete the following data from the NV store, application storage, and built-in media storage:

- all BlackBerry device user data
- any references to your organization's PIN encryption key
- any references to the device transport key
- if applicable, authentication information (for example, the binding information of the smart card)
- IT policy public key
- if you reset the device to the factory default settings, any references to past hashes of the device password
- record of time that elapsed since the user last turned on the device

- if you reset the device to the factory default settings, the IT policy that is stored on the device
- if a user selects the Include third party applications option or the User Installation Application option on the device, all third-party applications and application data

If you or a user turned on content protection, the device uses a memory-scrub process to overwrite the application storage on the device and built-in media storage. The memory-scrub process complies with United States government requirements for deleting sensitive user data, including *US Department of Defense Directive 5220.22-M* and *NIST Special Publication 800-88*.

For BlackBerry Device Software 5.0 and later, if you configure the Media Card Format on Device Wipe IT policy rule, the device can delete all user data from a media card. By default, the user can choose to delete third-party applications and the user data on the media card when the user permanently deletes all device data.

When a device deletes all device data

The BlackBerry device is designed to delete all device data from the device storage space when any of the following events occurs:

- The user clicks Wipe Device, Wipe Handheld, or Security Wipe in the security options on the device.
- The user types the device password incorrectly more times than the Set Maximum Password Attempts IT policy rule or the password option on the device permits. The default value is ten attempts.
- The user runs the application loader tool and types the device password incorrectly more times than the Set Maximum Password Attempts IT policy rule permits.
- The user uses the application loader tool to delete all user data and application data on the device. The user can choose not to delete the device applications.
- You send the Delete all device data and remove device IT administration command to the device with or without a delay (in hours), to the device. The maximum delay is 168 hours (7 days).
- You click the Remove user data from current device option in the BlackBerry Administration Service after you connect the device to the BlackBerry Administration Service. This option deletes all data and applications from the device even if service books do not exist on the device.

For more information about the security options on the device, see the user guide for the device.

Using IT policy rules to specify when a device must delete device data

You can configure the following IT policy rules to require that a BlackBerry device automatically deletes device data after a specific time or under specific conditions.

IT policy rule	Description
Secure Wipe Delay After IT Policy Received	This rule specifies the length of time (in hours) after a device receives an IT policy update or the Delete all device data and remove device IT administration command before the device deletes all BlackBerry device user data.
Secure Wipe Delay After Lock	This rule specifies the length of time (in hours) after a device locks before the device deletes all user data.
Secure Wipe if Low Battery	This rule specifies whether a device deletes all user data if the battery power level is low enough that the BlackBerry device turns off the wireless transceiver.

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Resetting a device to factory default settings

When a BlackBerry device resets to the factory default settings, the device overwrites the device storage space. If you or a BlackBerry device user turned on content protection, the device also uses a memory-scrub process to overwrite the application storage on the device and built-in media storage. When the device runs the memory-scrub process, it deletes any residual unmapped data.

You can use the Reset to Factory Defaults on Wipe IT policy rule to require that a device reset to the factory default settings when the device receives the Delete all device data and remove device IT administration command over the wireless network. When you change the value for the IT policy rule to Yes and send the IT administration command to the device, the device resets to the factory default settings and permanently deletes all applicable device data from the device storage space. If the device is running BlackBerry Device Software 4.5 or later, the device also deletes the Reset to Factory Defaults on Wipe IT policy and removes third-party applications.

If the device is running BlackBerry Device Software 4.5 or later and you change the value for the IT policy rule to Yes, the device resets to factory default settings when you send the IT administration command, when the user permanently deletes device data, or when the user exceeds the maximum number of times the user can try to type the device password.

Data flow: Deleting all device data from a device

When you delete all BlackBerry device data from a device using the Delete all device data and remove device IT administration command, the device performs the following actions:

1. Adds a Device Under Attack flag to the NV store

   If a user removes the battery or the battery power drops to zero before the device deletes all data, when the user replaces the battery, the process continues because the Device Under Attack flag is still present.

2. Restarts
3. Deletes the IT policy public key from the NV store to remove the binding between the device and the BlackBerry Enterprise Server

The device can bind to another BlackBerry Enterprise Server at a later time. The device does not use the memory-scrub process to overwrite the IT policy public key because it is not a protected or hidden value.

4. If applicable, deletes authentication information from the NV store

   For example, the device deletes the binding information for the smart card. The device can bind to another smart card at a later time.

5. Deletes data in the persistent store in application storage, including references to the device transport key and the copy of the principal encryption key
6. If you or a BlackBerry device user turned on content protection, overwrites the copy of the principal encryption key with zeroes
7. If applicable, formats the built-in media storage on the device
8. Overwrites the application storage with zeroes
9. Deletes the device password from the NV store
10. If you or a user turned on content protection, the memory-scrub process overwrites the file system of the device application storage and built-in media storage

    The memory-scrub process overwrites the device heap in RAM, which changes the state of each bit four times.

11. If you or a user specified that the data on the media card must be deleted, the memory-scrub process overwrites the media card
12. Deletes the Device Under Attack flag from the NV store

Scrubbing the memory of a device when deleting all device data

When you or a user deletes all BlackBerry device data for a device when content protection is turned on, the device runs the memory scrub process to overwrite the device heap that is in RAM, the flash memory, and the files that a user saved on the device.

Scrubbing the device heap in RAM when deleting all device data

To overwrite the BlackBerry device heap that is in RAM for a device when content protection is turned on, the device changes the state of each bit four times. The memory scrub process for a device performs the following actions:

1. writes 0x33 to each byte ($0011\ 0011_2$)
2. writes all bytes to 0x00 ($0000\ 0000_2$)

3. writes 0xCC to each byte (1100 1100_2)
4. writes all bytes to 0x00 (0000 0000_2)
5. writes 0x55 to each byte (0101 0101_2)
6. writes all bytes to 0x00 (0000 0000_2)
7. writes 0xAA to each byte (1010 1010_2)

Scrubbing the flash memory on a device when deleting all device data

For a BlackBerry device that is running BlackBerry Device Software version 4.6 or later and that has content protection turned on, the memory scrub process overwrites the NAND flash memory by writing a single character before it deletes the data. The memory scrub process writes 0x00 to each byte (0000 0000_2). The memory scrub process deletes all blocks and changes all bytes to 0xFF (1111 1111_2).

For a device that is running a version of BlackBerry Device Software that is earlier than version 4.6 and that has content protection turned on, the memory scrub process overwrites the NOR flash memory by changing the state of each bit four times. The memory scrub process performs the following actions:

1. writes 0x33 to each byte (0011 0011_2)
2. writes all bytes to 0xFF to each byte (1111 1111_2)
3. writes 0xCC to each byte (0x1100 1100_2)
4. writes all bytes to 0xFF (1111 1111_2)
5. writes 0x55 to each byte (0x0101 0101_2)
6. writes all bytes to 0xFF (1111 1111_2)
7. writes 0xAA to each byte (0x1010 1010_2)
8. writes all bytes to 0xFF (1111 1111_2)

Scrubbing the user files on a device when deleting all device data

If a BlackBerry device supports a partition of flash memory to store files that a user saved to the on-board device memory and you or a user turned on content protection, the memory scrub process overwrites that section of the device memory by writing a single character before the memory scrub process deletes the data. The memory scrub process performs the following actions:

1. writes 0x55 to each byte (0101 0101_2)
2. writes 0xAA to each byte (1010 1010_2)
3. deletes all blocks, and changes all bytes to 0xFF (1111 1111_2) or 0x00 (0000 0000_2)

7 Securing devices in your organization's environment for personal use and work use

Your organization might want to permit BlackBerry device users to use BlackBerry devices for both personal use and work use. For example, your organization might want to permit users to activate personal devices on a BlackBerry Enterprise Server or permit users to use devices that your organization purchases for personal use.

If devices are running a BlackBerry Device Software version that can distinguish between personal data and work data, security features and options on the devices allow the devices to treat your organization's data and applications differently from personal data and applications. The features and options have the following benefits:

- permit your organization to control access to your organization's data and applications on the devices
- help prevent your organization's data from being compromised
- provide a unified experience for users when they access personal data and work data
- permit your organization to delete your organization's data and applications from personal devices when users are no longer a part of your organization

How a device classifies what data and applications are for work use or personal use

To control what happens to your organization's data and applications on a BlackBerry device, you can configure a device to distinguish between data and applications that are for personal use and data and applications that are for work use. You must set the Enable Separation of Work Content IT policy rule to Yes before the device can distinguish between work data and personal data.

By default, after you configure the Enable Separation of Work Content IT policy rule, core applications can access work data, personal data, or both. For example, the email application can access both work data and personal data because a BlackBerry device user can use the email application to manage the work email account and personal email accounts. To determine whether a third-party application or an add-on application developed by Research In Motion can access work

data, you must configure the "Is access to the corporate data API allowed" application control policy rule. The device checks this rule to determine which applications can access work data.

After you configure the Enable Separation of Work Content IT policy rule, the following events can occur:

- the device and BlackBerry Enterprise Server do not synchronize personal organizer data
- an application can determine whether it can access work data
- after applications that can access work data register with the device, the applications can delete work data without deleting personal data when the device notifies the applications that they must delete work data

To help a device determine which data is work data, you can provide the device with domain information for your organization. You can specify a list of domain names, email address domains, and certificate server domains that are specific to your organization in the Work Domains IT policy rule. For example, if a user sends an email message to a contact that is not in the contact list on the device, the device can use the domain information in the Work Domains IT policy rule to determine whether the contact is a work contact.

Data and applications that a device classifies for work use

A BlackBerry device classifies the following data and applications for work use:

- email messages and attachments that are sent to the BlackBerry device user's work email account and the email messages and attachments that the user sends from the work email account
- draft email messages that the user creates using their work email account
- calendar entries that the user creates using their work calendar
- contacts that the BlackBerry Enterprise Server synchronizes with the user's work email account
- organizer data, such as tasks and memos
- applications that you send to the device from a BlackBerry Enterprise Server, and that have the "Is access to the corporate data API allowed" application control policy rule set to Allow
- files that the user accesses and downloads from your organization's network using the Files application
- files on media cards that are created by applications that can access work data (except for media applications)

The BlackBerry device classifies email addresses in the user's contact list as work email addresses using the domains that you specify in the Work Domains IT policy rule.

After the device classifies data for work use, the user cannot reclassify the data for personal use. For example, if a user selects a work email account in the Send Using field of a draft email message and starts typing a message in the body, the user cannot change the selected work email account to a personal email account. However, the user can reclassify personal data as work data. For example, if the user selects a personal email account in the Send Using field of a draft email message, the user can change the selected personal email account to a work email account even after they start typing a message in the body of the email.

Data and applications that a device classifies for personal use

A BlackBerry device classifies the following data and applications for personal use:

- email messages and attachments that a BlackBerry device user sends from any email account (for example, a personal email account) except for the work email account
- contacts that the device synchronizes with personal email accounts (for example, Google Mail contacts)
- phone data (phone data is considered to be personal data but the call history and call logs are deleted when you delete work data)
- instant messages that a user sends or receives using BlackBerry Messenger
- text messages that a user sends or receives using PIN messaging, SMS text messaging, or MMS messaging
- applications that have the "Is access to the corporate data API allowed" application control policy rule set to Deny
- content that is stored for the BlackBerry Browser (the BlackBerry Browser is a personal application but the cache is deleted when you delete work data)
- maps
- media application data (for example, the camera, video, music, or voice recorder)
- passwords that the Password Keeper encrypts

Preventing a user from compromising work data on a device

A BlackBerry device is designed to separate work data from personal data so that you can help prevent a BlackBerry device user from compromising your organization's data by using personal channels to unintentionally send work data. You can configure several features to help prevent a user from compromising your organization's data on a device:

- prevent a user from pasting work data into a personal application
- prevent a user from forwarding work data using a personal channel
- prevent a user from using the work contact list in personal email accounts and personal calendars
- prevent a user from backing up work data
- control the browser traffic in BlackBerry Browser
- protect the work data that a user stores on a media card

Preventing a user from pasting work data into a personal application

To help prevent a BlackBerry device user from pasting work data into a personal application, you can set the Enable Separation of Work Content IT policy rule to Yes so that the following guidelines apply to the user:

- a user can cut, copy, and paste work data from a work application to another work application
- a user cannot cut, copy, and paste work data from a work application to a personal application
- a user can cut, copy, and paste personal data from a personal application to a work application or another personal application

If a user tries to paste work data to a personal application, the BlackBerry device displays a warning message.

By default, the Enable Separation of Work Content IT policy rule is set to No. The device does not distinguish between work data and personal data.

If you set the Enable Separation of Work Content IT policy rule to Yes, a user can select a work email account in the Send Using field of a draft email message, paste work data into the body of the email message, and then change the selected work email account in the Send Using field to a personal email account before the user sends the email message. If you would like to prevent the user from changing the work email account to a personal email account, you should also set the Require Work Resources For Conducting Work Activities IT policy rule to Yes. By default, the Require Work Resources For Conducting Work Activities IT policy rule is set to No.

Preventing a user from forwarding work data using personal channels

To help prevent a BlackBerry device user from forwarding work data using personal channels, you can set the Disable Forwarding of Work Content Using Personal Channels IT policy rule to Yes. Personal channels include the BlackBerry Internet Service, SMS text messages, MMS messages, PIN messages, and BlackBerry Messenger. When you set the Disable Forwarding of Work Content Using Personal Channels IT policy rule to Yes, the device permits the user to follow these guidelines:

- a user can forward work email messages, contacts, calendar entries, tasks, or memos using a work email account
- a user cannot forward work email messages, contacts, calendar entries, tasks, or memos using personal channels

If the user tries to forward work email messages, contacts, calendar entries, tasks, or memos using personal channels, the device is designed to display a warning message and does not permit the user to complete the task.

By default, the Disable Forwarding of Work Content Using Personal Channels IT policy rule is set to No. The device does not distinguish between work data and personal data when users forward data.

Prevent a user from using the work contact list in personal email accounts and personal calendars

By default, a BlackBerry device does not prevent a BlackBerry device user from using personal email accounts or personal calendars to send email messages or calendar appointments to email addresses in the work contact list. For example, a user can send email messages to work email addresses using a personal email account and create meetings with work email addresses in a personal calendar.

To help prevent a user from using personal email accounts or personal calendars to send email messages or calendar appointments to email addresses in the work contact list, you can set the Require Work Resources For Conducting Work Activities IT policy rule to Yes. When you set this rule to Yes, a user must use the work email account to send email messages to work email addresses and the work calendar to send calendar invites to work email addresses.

Controlling the browsing traffic in the BlackBerry Browser

A BlackBerry device user can use the BlackBerry Browser to browse the Internet and your organization's intranet. The device does not consider the BlackBerry Browser to be a work application. You can change the behavior of the BlackBerry Browser depending on the IT policies that you configure in your organization's environment:

- If you do not want users to browse using the Internet Browser, set the Allow IBS Browser IT policy rule to No.
- If you do not want users to browse using Wi-Fi hotspots, set the Allow Hotspot Browser IT policy rule to No.
- If you do not want users to browse using WAP, set the Enable WAP Config IT policy rule to No.
- If you want users to browse using only the BlackBerry Enterprise Server, set the Allow Other Browser Services IT policy rule to No.
- If you do not want users to browse using the BlackBerry Enterprise Server, set the Allow Browser IT policy rule to No.

You can also configure pull rules to prevent a user from accessing specific web servers using the BlackBerry Browser. For more information about configuring pull rules, see the *BlackBerry Enterprise Server Administration Guide*.

BlackBerry 6 permits you to control the browser transport selection for the BlackBerry Browser. For more information about browser transport selection, see the *Selecting Browser Transport Technical Note*.

Preventing a user from backing up work data that is stored on a device

By default, if your organization's environment includes BlackBerry Enterprise Server for Microsoft Exchange (5.0 SP3 or later) or BlackBerry Enterprise Server for IBM Domino (5.0 SP3 or later), a BlackBerry device user can back up both work

data and personal data on a computer using the BlackBerry Desktop Software and BlackBerry Web Desktop Manager. The user can restore the data to the device that the user backed up after the BlackBerry Device Software is updated or when issues occur that require the user to restore the information.

In rare circumstances, when a user restores work data, a device might not be able to recognize the data as work data and might treat it as personal data. For example, if a user restores data from an existing device to a new device that the user did not activate on the BlackBerry Enterprise Server and that has the radio turned off, the new device might not recognize the data as work data.

If you want to prevent the user from backing up work data, you can change the value of the Desktop Backup IT policy rule to No organizational databases. When you set the rule to No organizational databases, the device does not back up the following information:

- organizer data such as tasks or memos
- work contacts
- work calendar entries

Protecting work data on a media card

By default, a BlackBerry device stores all data in unencrypted format on a media card. When you set the Enable Separation of Work Content IT policy rule to Yes, the device automatically encrypts all work data on a media card using a device key.

You can perform any of the following actions to further protect the work data on a media card:

- Prevent a user from storing any data on media cards by setting the Disable External Memory IT policy rule to Yes.
- Prevent a user from transferring data to a media card over a USB connection by setting the Disable USB Mass Storage IT policy rule to Yes.
- Permit the user to store data on media cards, but specify that the device must encrypt all data and not just work data. To configure this option, set the External File System Encryption Level IT policy rule to one of the following values:
  - Encrypt to User Password (excluding multi-media directories)
  - Encrypt to User Password (including multi-media directories)
  - Encrypt to Device Key (excluding multi-media directories)
  - Encrypt to Device Key (including multi-media directories)
  - Encrypt to User Password and Device Key (excluding multi-media directories)
  - Encrypt to User Password and Device Key (including multi-media directories)

Deleting only work data from a device

To help protect your organization's data on a personal BlackBerry device, you can permit your organization to delete work data from a device when a user no longer works at your organization. You can use the BlackBerry Administration Service to

require that a personal device remove only work data when the device receives the Delete only the organization data and remove device IT administrative command over the wireless network. All personal data remains on the device. A BlackBerry device user cannot use the device or make emergency calls while the device deletes the work data.

The device permanently deletes the following work data:

Item	Description
email messages	• email messages that are sent to the user's work email account and the email messages that the user sends from the work email account • draft email messages that the user creates using their work email account
attachments	attachments that are sent to the user's work email account and the attachments that the user sends from the work email account
calendar entries	calendar entries that the user creates using their work calendar
contacts	contacts that the BlackBerry Enterprise Server synchronizes with the user's work email account
memos	all memos
tasks	all tasks
call history	although the device defines phone data for personal use, the call history entries are deleted when you delete work data
call logs	although the device classifies phone data as personal data, the call log files are deleted when you delete work data
the BlackBerry Browser cache	although the device specifies the BlackBerry Browser for personal use, the BlackBerry Browser cache is deleted when you delete work data
files	• files that the user accesses and downloads from your organization's network using the Files application • files on media cards that are created by applications that can access work data (except for media applications) • work data is not deleted from the media card if the media card is not available when the device deletes work data, however the user cannot access work data on the media card after the device removes work data
IT policy	IT policy that is associated with your organization
PIN encryption key	references to your organization's PIN encryption key
device transport key	references to the device transport key which prevents the device from communicating with the BlackBerry Enterprise Server
work service books	service books on the device that the device classifies for work use

Data flow: Deleting only work data from a device

When you delete only work data from a BlackBerry device using the Delete all organizational device data IT administration command, the device performs the following actions:

1. Adds a Corporate Device Under Attack flag to the NV store

   If a user removes the battery or the battery power drops to zero before the device deletes all work data, when the user replaces the battery, the process continues because the Corporate Device Under Attack flag is still present.

2. Displays a notification that the device will begin deleting work data in 2 minutes

   If a user removes the battery or the battery power drops to zero before the process ends, when the user replaces the battery, the process of deleting work data continues but the device does not display a notification that the device will begin deleting work data.

3. Turns off the wireless transceiver
4. Notifies any applications on the device (for example, the Messages application, Calendar application, and registered third-party applications) that manage work data that they must delete the work data that they are responsible for from the device. The applications then delete the work data that they manage on the device.

   Any applications on the device that manage work data must register with the device to receive a notification from the device when they must delete the work data that they are responsible for. If applications on the device that manage work data do not register with the device, the work data that they are responsible for may not be deleted.

5. Deletes all device transport keys
6. Sends an acknowledgement to the BlackBerry Enterprise Server that the work data was successfully deleted from the device
7. Displays a notification that the device successfully removed work data from the device and that the device is going to restart
8. Restarts
9. Deletes the IT policy public key from the NV store to remove the binding between the device and the BlackBerry Enterprise Server which terminates its connection with the BlackBerry Enterprise Server

   The device can bind to another BlackBerry Enterprise Server at a later time. The device does not use the memory-scrub process to overwrite the IT policy public key because it is not a protected value or hidden value.

10. Deletes the Corporate Device Under Attack flag from the NV store
11. Sends an IT policy change notification to all applications so that applications that depend on the IT policy can make changes if required

Managing third-party applications on a smartphone that a user uses for personal purposes

By default, a BlackBerry smartphone classifies all applications as work applications that can access work data.

After you set the Enable Separation of Work Content IT policy rule to Yes, if you do not want specific third-party applications to access work data such as work contacts, you can consider performing any of the following actions:

- Create a software configuration for all unlisted applications and set the "Is access to the corporate data API allowed" application control policy rule to Deny. This prevents all third-party applications from accessing work data. If you want to allow specific third-party applications to access work data, you can create a software configuration that allows only third-party applications that you specify to access work data.
- Create a software configuration for each application that you want to prevent from accessing work data and set the "Is access to the corporate data API allowed" application control policy rule to Deny. This prevents third-party applications that you specify from accessing work data and allows all third-party applications that you do not specify to access work data.
- Create a software configuration and set the disposition for unlisted applications to Disallowed. This prevents a BlackBerry smartphone user from installing any third-party applications on the smartphone that you did not specifically list in the software configuration.
- Create a software configuration that lists specific applications and set the disposition to Disallowed. This prevents a user from installing the third-party applications that you listed in the software configuration.

For more information, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Enterprise Server Administration Guide*.

Managing add-on applications on a device that a user uses for personal purposes

By default, a BlackBerry device classifies all add-on applications developed by Research In Motion as work applications that can access work data.

After you set the Enable Separation of Work Content IT policy rule to Yes, if you do not want add-on applications to access work data such as work contacts, you can use existing IT policy rules to prevent the applications from accessing work data. For example, you can set the Disable Organizer Data Access for Social Networking Applications IT policy rule to Yes to

prevent add-on applications such as Facebook for BlackBerry smartphones and MySpace for BlackBerry smartphones from accessing the work calendar and work contact list.

The Enable Separation of Work Content IT policy rule has some effect on add-on applications. For example, if you set the Enable Separation of Work Content IT policy rule to Yes, the Facebook application prevents users from pasting work data.

To prevent add-on applications developed by RIM from accessing work data, the "Is access to the corporate data API allowed" application control policy rule for the applications must be set to Deny. If this application control policy rule is not set to Deny, users can copy and paste work data into the applications.

For more information about which applications are add-on applications developed by RIM, browse to www.blackberry.com/support to read KB24317.

IT policy rules that apply to devices that users use for personal purposes

The following IT policy rules apply to BlackBerry devices that BlackBerry device users use for personal purposes:

IT policy group	IT policy rule
Browser	• Allow Hotspot Browser • Allow IBS Browser
Device Only	Enable WAP Config
Global	Allow Browser
Personal Devices	• Disable Forwarding of Work Content Using Personal Channels • Enable Separation of Work Content • Require Work Resources for Conducting Work Activities • Work Domains
Security	• Desktop Backup • Disable External Memory • Disable USB Mass Storage • External File System Encryption Level

For more information about the IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Protecting data on a device

8

Encrypting user data on a locked device

If you or a BlackBerry device user turns on content protection, you or the user can configure a locked device to encrypt stored user data and data that the locked device receives. When you or a user turns on content protection, a locked device is designed to use AES-256 encryption to encrypt stored data and an ECC public key to encrypt data that the locked device receives.

For example, the locked device uses content protection to encrypt the following items:

- subject, location, meeting organizer, attendees, and any notes in all appointments or meeting requests
- all contact information in the contact list except for the contact title and category
- subject, email addresses of intended recipients, message body, and attachments in all email messages
- title and information that is included in the body of a note for all memos (also known as posted messages)
- subject and all information that is included in the body of tasks (also known as posted all day appointments)
- if you use software tokens, contents of the .sdtid file seed that is stored in flash memory
- all data that is associated with third-party applications that a user installs on the device
- in the BlackBerry Browser, content that web sites or third-party applications push to the device, any web sites that the user saves on the device, and the browser cache
- all text that replaces the text automatically that the user types on the device

You can change the Content Protection of Contact List IT policy rule to Required to prevent the user from turning off content protection for the contact list on the device. If you change the Content Protection of Contact List IT policy rule to Required, the device does not permit call display and does not share contacts over a Bluetooth connection when the device is locked.

Configuring the encryption of device data on a locked device

You can turn on content protection of BlackBerry device data on a locked device using the Content Protection Strength IT policy rule. You can choose a strength level that corresponds to the ECC key strength that your organization requires.

A user can turn on content protection in the security options, in the encryption options on the device. The user can change the content protection strength to the same level that you specify using the IT policy rule or to a higher level.

To make content protection optional or to prevent an administrator or a user from turning on content protection for a device that is running BlackBerry Device Software 6.0 or later, you can use the Content Protection Usage IT policy rule.

After you or a user configures content protection, a device uses the ECC private key to decrypt an email message that it received when it was locked. The longer the ECC private key, the more time the device requires to decrypt messages. You must choose a strength level that optimizes the encryption strength or that optimizes the decryption process.

The device uses the device password to generate an ephemeral key that the device uses to encrypt the content protection key and ECC private key. If you change the content protection strength to Stronger so that the device uses a 283-bit ECC private key, you can consider changing the Minimum Password Length IT policy rule to enforce a minimum password length of 12 characters for the device password. If you change the content protection strength to Strongest so that the device uses a 571-bit ECC private key, you can consider changing the Minimum Password Length IT policy rule to enforce a minimum password length of 21 characters for the device password. These password lengths maximize the encryption strength that the longer ECC private keys are designed to provide. A shorter password length produces a weaker ephemeral key.

Data flow: Encrypting user data on a locked device

When a BlackBerry device locks for the first time after you or a user turns on content protection, the device performs the following actions:

1. uses the content protection key to automatically encrypt the bulk of its stored user data and application data
2. frees the device memory that is associated with the decrypted content protection key and the decrypted ECC private key that is stored in RAM
3. uses the ECC public key to encrypt data that it receives

Data flow: Decrypting user data on an unlocked device

1. A user types the correct BlackBerry device password to unlock a device.
2. The device performs the following actions:
   a. uses the password to derive the ephemeral key
   b. uses the ephemeral key to decrypt the encrypted content protection key and ECC private key that are stored in flash memory
   c. stores the decrypted content protection key and ECC private key in RAM
   d. uses the decrypted content protection key to decrypt the user data when the user tries to access user data (for example, an email message) that the device received and encrypted while it was locked
   e. uses the decrypted ECC private key to decrypt the user data and access the ECC-encrypted items (for example, the message body, subject, or recipient) when the user tries to access user data that the device encrypted while it was locked

When the device opens ECC-128 encrypted items (usually less than 40 messages), the device uses the ECC private key to decrypt the ECC-encrypted items. The device re-encrypts the items with the content protection key the next time that the

device locks. If the device does not complete the re-encryption process before the user unlocks the device, the device resumes re-encryption when it locks again.

Encrypting the device transport key on a locked device

If you turn on content protection for device transport keys, a BlackBerry device uses the principal encryption key to encrypt the device transport keys that are stored in flash memory. The device encrypts the principal encryption key using the content protection key. When a locked device receives data that is encrypted using the device transport key, it uses the decrypted principal encryption key to decrypt the device transport key in flash memory and then uses the decrypted device transport key to decrypt data.

When you, a user, or a password timeout locks the device, the wireless transceiver remains on and the device does not delete the memory that is associated with the principal encryption key or device transport key. The device is designed to prevent the decrypted principal encryption key and the decrypted device transport key from appearing in flash memory.

You can turn on content protection for device transport keys on the device when you configure the Force Content Protection of Master Keys IT policy rule. When you turn on content protection of device transport keys, the device uses the ECC key strength that you specified in the Content Protection Strength IT policy rule to encrypt the device transport keys.

What happens when a user resets a device after you turn on content protection for the device transport key

If you turn on content protection of device transport keys, a BlackBerry device performs the following actions when a user resets the device by removing and reinserting the battery:

- turns off the data connection over the wireless network
- suspends serial bypass connections if your organization's environment includes an enterprise Wi-Fi network and the device can connect directly to a BlackBerry Router
- frees the memory that is associated with all data and keys, including the decrypted principal encryption key
- locks itself

The device is designed to turn off the data connection and serial bypass connection while the content protection key is unavailable to decrypt the principal encryption key in flash memory. Until a user unlocks the device, the device cannot receive and decrypt data. The device does not turn off the wireless transceiver and can still receive phone calls, SMS text messages, and MMS messages.

When the user unlocks the device after resetting it, the device performs the following actions:

- uses the content protection key to decrypt the principal encryption key in flash memory
- stores the decrypted principal encryption key in flash memory

- connects to the BlackBerry Infrastructure
- resumes serial bypass connections
- receives data from the BlackBerry Enterprise Server

Resetting a device password when content protection is turned on

If you or a BlackBerry device user turns on content protection for a BlackBerry device that is running BlackBerry Device Software version 4.3 or later, you can reset the device password using a BlackBerry Enterprise Server version 4.1 SP5 or later. The BlackBerry Enterprise Solution uses the remote password reset cryptographic protocol to reset the device password when content protection is turned on. The device does not prompt the user for the old device password.

The remote password reset cryptographic protocol is designed to provide the following features:

- permit the device to encrypt the content protection key again with the new password, without the old password being available
- prevent a hardware-based attack on the device from recovering the content protection key without knowing either the device password or the IT policy private key that the BlackBerry Enterprise Server generates for the device
- prevent the BlackBerry Enterprise Server from accessing any data that a potentially malicious user could use to recover the content protection key

To reset the device password, you send the Specify new device password and lock device IT administration command to the device. You should send the IT administration command to a content-protected device that is in the possession of the user only. If you send the IT administration command to a device that is in the possession of a potentially malicious user, that user can use a hardware-based attack to recover the key pair that the device created when it received the IT policy. The potentially malicious user can use the key pair to decrypt all the data on the device.

Data flow: Resetting a device password when content protection is turned on

The process flow is designed so that the BlackBerry Enterprise Server cannot reconstruct the encryption key at a later time.

The BlackBerry Enterprise Server performs the following actions when you send the Specify new device password and lock device IT administration command to a BlackBerry device when content protection is turned on:

1. generates an encryption key using the IT policy public key and the NIST recommended 521-bit elliptic curve over a prime field
2. encrypts the content protection key using the encryption key and the new device password (which is also encrypted)
3. sends the data required to reconstruct the encryption key to the device

Cryptosystem parameters that the remote password reset cryptographic protocol uses

The BlackBerry Enterprise Server and BlackBerry device are designed to share the following cryptosystem parameters when they use the remote password reset cryptographic protocol.

Uppercase parameters represent elliptic curve points. Lowercase parameters represent scalars. The elliptic curve group operations are additive.

Parameter	Description
E(Fq)	This parameter represents the NIST approved 521-bit random elliptic curve over *Fq*, which has a cofactor of 1.
Fq	This parameter represents a finite field of prime order q.
P	This parameter represents a point of E that generates a prime subgroup of *E(Fq)* of order p.
B = bP	This parameter represents the long-term IT policy public key and IT policy private key pair that the BlackBerry Enterprise Server generates for the BlackBerry device. The BlackBerry Enterprise Server stores *b* in the BlackBerry Configuration Database and sends *B* to the BlackBerry device in the IT policy.
D = dP	This parameter represents the key pair that the BlackBerry device creates when it receives *B*. The BlackBerry device stores *D*, but it deletes *d* to prevent a hardware-based attack from recovering *d* and *B* and then calculating *K = dB*.
K = dB	This parameter represents the encryption key that the BlackBerry device uses to encrypt the content protection key.
r	This parameter represents a short-term random number that the BlackBerry device stores in RAM.
D' = rD	This parameter represents a blinded version of *D*.
K' = bD' = brD = rK	This parameter represents a blinded version of *K*.

Protecting passwords that a device stores

A BlackBerry device user can use the password keeper to store all passwords that the user uses to access applications and web sites from a BlackBerry device. The password keeper is designed to protect the passwords with a password keeper password. The user is required to remember only the password keeper password.

The first time that the user opens the password keeper on the device, the user must create the password keeper password. The password keeper encrypts the information that it stores using AES-256 encryption, and uses the password keeper password to decrypt the information when the user types the password keeper password. The device deletes all device data if a user types the password keeper password incorrectly 10 times.

In the password keeper, a user can perform the following actions:

- type a password and its identifying information (for example, which application the user can access using the password), and save the information
- generate random passwords that are designed to improve password strength
- copy passwords and paste them into an application or password prompt for a web site

Protecting data that a device stores on a media card

To protect the data that a BlackBerry device stores on a media card, you can configure the External File System Encryption Level IT policy rule, or a user can configure the corresponding option on the device. You can use this rule or option to configure whether the device encrypts the data using a password that a user provides, a device key that is randomly generated and stored in the NV store, or both.

A media card can store a master key and the code-signing keys that are included in the header information of encrypted files. The code-signing keys permit only applications that signed the files to access the files. A device is designed to use the master key that is stored on the media card to decrypt and encrypt files on the media card. The master key and code-signing keys use AES encryption. The device is designed to check the code-signing keys when the device opens the input streams or output streams of an encrypted file and to use code-signing with RSA-1024 encryption to control access to objects on the media card.

When a user stores a file on a media card for the first time after you or the user turns on encryption of media cards, the device decrypts the encryption key for the media card file and uses it to encrypt the stored file. The device does not encrypt files that a user transfers to the media card using a USB mass storage device.

The device, a computer, and other devices that use the media card can modify encrypted files (for example, truncate files) on the media card. The device is not designed to perform integrity checks on data in encrypted files.

For more information, visit www.blackberry.com/go/serverdocs to read *Enforcing encryption of internal and external file systems on BlackBerry devices Technical Overview*.

Data flow: Generating an encryption key for a media card

When you or a user turns on encryption of media cards for the first time, a BlackBerry device generates an encryption key (also known as a session key) for a media card.

To generate an encryption key, the BlackBerry device performs the following actions:

1. generates an AES-256 encryption key
2. stores the encryption key in the NV store in RAM on the BlackBerry device
3. XORs the AES-256 encryption key with another AES-256 encryption key that is encrypted with a password to generate the encryption key for the media card
4. encrypts the encryption key for the media card using the AES-256 encryption key
5. stores the encrypted encryption key for media cards on the media card

How the BlackBerry Attachment Service protects data on a device

A BlackBerry device uses the BlackBerry Attachment Service to process an attachment in an email message or calendar entry so that the user can view the attachment on the device. The BlackBerry Attachment Service is designed to prevent a potentially malicious application from accessing data on the device by using binary format parsing to open the attachment and process it.

After the BlackBerry Attachment Service processes the attachment, the BlackBerry Router sends the attachment to the device for rendering. If the attachment in the email message or calendar entry is an application, the device does not run the application.

For more information about the attachment file formats that the BlackBerry Enterprise Server supports, see the *BlackBerry Enterprise Server Feature and Technical Overview*.

Best practice: Protecting the BlackBerry Attachment Service

To help prevent the spread of potential attacks from the computer that hosts the BlackBerry Attachment Service to other computers in your organization's network, consider the following guidelines:

- Install the BlackBerry Attachment Service on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server.
- Place the computer that hosts the BlackBerry Attachment Service in its own network segment.

How a device protects its operating system and the BlackBerry Device Software

Each time a user turns on a BlackBerry device, specific components on the device automatically check the authenticity of the device operating system and the integrity of the BlackBerry Device Software. The BlackBerry Device Software must pass these security checks before the user can run the BlackBerry Device Software and before the user can update the BlackBerry Device Software over the wireless network.

How a device authenticates the boot ROM code and binds the device processor when the device turns on

A BlackBerry device processor provides an authentication method that is designed to verify that the boot ROM code is permitted to run on a device. The manufacturing process installs the boot ROM code in flash memory on the device. The boot ROM code is the root of trust on devices. The RIM signing authority system, which signs the boot ROM code for a device during the manufacturing process, uses an RSA public key to sign the boot ROM code. The processor is configured during the manufacturing process to store information that the processor can use to verify the digital signature of the boot ROM code.

When a user turns on a device, the processor runs internal ROM code that reads the boot ROM from flash memory and verifies the digital signature of the boot ROM code using the RSA public key. If the verification process is successful, the boot ROM is permitted to run on the device. If the verification process is not successful, the processor stops running.

The process of binding a processor to a boot ROM can occur when the processor is manufactured, the device is manufactured, or the BlackBerry Device Software is configured, depending on the manufacturer and model number of the processor.

Protecting the data that the BlackBerry Enterprise Server stores in your organization's environment

9

Where the BlackBerry Enterprise Server stores messages and user data in the messaging environment

The BlackBerry Enterprise Server stores the messages and user data for a BlackBerry device in the messaging environment so that the BlackBerry Enterprise Server can maintain a connection between a user's email account and the device. To avoid compromising the user data that is stored in the messaging environment, you must protect the storage location in the messaging environment.

Messaging environment	Storage location
IBM Domino	The following Domino databases store data for the BlackBerry Enterprise Server: • The BlackBerry state database stores an entry that opens a connection between each original email message in a user's IBM Notes Inbox and the same email message on the user's device. Each user account has a uniquely named BlackBerry state database. • The BlackBerry profiles database stores configuration information for each user account, including the identification information for the device and the device transport key. The BlackBerry profiles database stores a link to a BlackBerry state database and stores other information that the BlackBerry Enterprise Server uses to manage how email messages are sent to and from the device.

Messaging environment	Storage location
Microsoft Exchange	The BlackBerry Enterprise Server stores user data in hidden folders in the Microsoft Exchange mailbox for the user.
Novell GroupWise	The BlackBerry Enterprise Server stores user data in the POA where the user account is located.

Data that the BlackBerry Configuration Database stores

The BlackBerry Configuration Database stores the following information:

- name of each BlackBerry Enterprise Server
- unique SRP authentication keys and unique SRP IDs, or UIDs, that each BlackBerry Enterprise Server uses in the SRP authentication process to open a connection to the wireless network
- IT policy private keys of the IT policy key pairs that the BlackBerry Enterprise Server generates for each BlackBerry device
- PIN of each device
- read-only copies of each device transport key
- copy of your organization's user directory
- a semi-permanent reference to user data using the Novell GroupWise MessageID in the database synchronization tables that are named MBMailSync, MBCalendarSync, MBPIMSync, and MBFolderSync (BlackBerry Enterprise Server for Novell GroupWise only)

The BlackBerry Enterprise Server components that do not connect to a messaging server can access the information that the BlackBerry Configuration Database stores.

Best practice: Protecting the data that the BlackBerry Configuration Database stores

Best practice	Description
Audit connections to the Microsoft SQL Server.	Consider the following guidelines:

Best practice	Description
	• At a minimum, write failed connection attempts to the Microsoft SQL Server log file and review the log file regularly. • When possible, save log files to a different hard disk drive than the one that the data files are stored on.
Delete unsecured, old setup files.	Consider deleting Microsoft SQL Server setup files that might contain plaintext, credentials encrypted with weak public keys, or sensitive information that the Microsoft SQL Server logged to a Microsoft SQL Server version-dependent location during the Microsoft SQL Server installation process. Microsoft distributes the Killpwd tool, which is designed to locate and delete passwords from unsecured, old setup files in your organization's environment. For more information, visit www.support.microsoft.com to read article KB263968.
Limit the permission level of the Microsoft SQL Server.	Consider associating each Microsoft SQL Server service with a Windows account that the service derives its security context from. Microsoft SQL Server permits the sa account and, in some cases, other user accounts to access operating system calls based on the security context of the account that runs the Microsoft SQL Server service. If you do not limit the permission level of the Microsoft SQL Server, an attacker might use these operating system calls to attack any other resource that the account has access to.
Make the Microsoft SQL Server port numbers that are monitored by default on your organization's firewall unavailable.	Consider configuring your organization's firewall to filter packets that are addressed to TCP port 1433, addressed to UDP port 1434, or associated with named instances.
Protect the sa account using a password.	Consider assigning a password to the sa account on the Microsoft SQL Server, even on servers that require Windows authentication. The password is designed to prevent an empty or weak password for the sa account from being exposed if an administrator of the database resets the Microsoft SQL Server for mixed mode authentication.
Protect the Microsoft SQL Server installation from Internet-based attacks.	Consider the following guidelines: • Require Windows Authentication Mode for connections to the Microsoft SQL Server to restrict connections to Windows user accounts and domain user accounts, and turn on credentials delegation. Windows Authentication Mode does not require you to store passwords on the computer. • Use stronger authentication protocols, required password complexity, and required expiration times.
Use a secure file system.	Consider the following guidelines:

Best practice	Description
	• Use NTFS for the Microsoft SQL Server because it is more stable and recoverable than FAT file systems, and NTFS permits security options such as file and directory ACLs and EFS. • Do not change the permissions that the Microsoft SQL Server specifies during the Microsoft SQL Server installation process. The Microsoft SQL Server creates appropriate ACLs on registry keys and files if it detects NTFS. • If you must change the account that runs the Microsoft SQL Server, decrypt the files that you could access using the old account and encrypt them again for access using the new account.
Use Microsoft SQL Server Management Studio.	Consider the following guidelines: • Use Microsoft SQL Server Management Studio to change the account that is associated with a Microsoft SQL Server service, if required. Microsoft SQL Server Management Studio configures the appropriate permissions on the files and registry keys that the Microsoft SQL Server uses. • Do not use the Microsoft Management Console Services applet to change the account that is associated with a Microsoft SQL Server service. To use this applet, you must manually change the Windows registry, the permissions for the NTFS file system, and Windows user rights. For more information, visit www.support.microsoft.com to read article KB283811.

How the BlackBerry Enterprise Server and device protect IT policies

After the BlackBerry Enterprise Server installation process creates the BlackBerry Configuration Database, the BlackBerry Enterprise Server generates an IT policy key pair that it can use to authenticate and protect the IT policy. When you assign a BlackBerry device to the user account and activate the device, the BlackBerry Enterprise Server sends the IT policy and the IT policy public key to the device.

The BlackBerry Enterprise Server stores the IT policy private key in the BlackBerry Configuration Database. The BlackBerry Enterprise Server uses the IT policy private key to digitally sign all data packets that include IT policy data when the BlackBerry Enterprise Server sends the IT policy to the device. The device uses the IT policy public key in the NV store to authenticate the digital signature on the IT policy.

A device stores the digitally signed IT policy and the IT policy public key in the NV store in flash memory. When the device stores the IT policy and IT policy public key, the device binds the IT policy to itself so that the device can use the IT policy to control its behavior.

Protecting communication with a device

10

Opening a direct connection between a device and a BlackBerry Router

A BlackBerry device can use the BlackBerry Router protocol to bypass the SRP-authenticated connection to the BlackBerry Infrastructure and open a direct connection to a BlackBerry Router. The device can open a direct connection to the BlackBerry Router if a BlackBerry device user connects the device to a computer that hosts the BlackBerry Device Manager. A device can also open a direct connection to the BlackBerry Router over an enterprise Wi-Fi network using port 4101. A direct connection between the BlackBerry Router and device is referred to as least-cost routing because it eliminates the cost of using the BlackBerry Infrastructure.

Before the BlackBerry Enterprise Server and device can send any data to each other, the device must authenticate with the BlackBerry Enterprise Server by verifying the device transport key. The device opens an authenticated connection to the BlackBerry Router after the device authenticates with the BlackBerry Enterprise Server. The BlackBerry Router does not know the value of the device transport key that the BlackBerry Enterprise Server and device share.

If the device connects to the BlackBerry Router over the enterprise Wi-Fi network, after the BlackBerry Router opens an authenticated connection, the BlackBerry Router communicates with the device over the enterprise Wi-Fi network using port 4101. If you do not configure the BlackBerry Router to connect only to a Wi-Fi network, the BlackBerry Router verifies that the PIN belongs to a device that is registered with the BlackBerry Infrastructure.

If you want the BlackBerry Router and device to use the BlackBerry Router protocol, you can consider installing the BlackBerry Router on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server to prevent a potentially malicious attacker from having direct access to the computer that hosts the BlackBerry Enterprise Server. If the BlackBerry Router is placed in the DMZ, you must open port 4101 on the internal-facing firewall to permit communication between the BlackBerry Device Manager and BlackBerry Router.

Advantages of using the BlackBerry Router protocol

You can use the BlackBerry Router protocol to experience the following advantages:

- You or a BlackBerry device user can connect multiple BlackBerry devices to a single computer that hosts a BlackBerry Device Manager.
- The BlackBerry Router rejects connections from devices that the BlackBerry Enterprise Server has not authenticated.

- A device can provide all email messaging services and data services using the BlackBerry Router protocol except for activation over the wireless network. After a user starts the activation process over the wireless network, the user can connect the device to a computer that hosts the BlackBerry Device Manager to complete the activation process.

Data flow: Authenticating a device with the BlackBerry Enterprise Server using the BlackBerry Router protocol

1. A user connects a BlackBerry device to a computer that hosts the BlackBerry Device Manager or connects a device to an enterprise Wi-Fi network.
2. The BlackBerry Enterprise Server and device use the BlackBerry Router protocol to verify that the device knows the device transport key.

   The BlackBerry Router protocol uses two runs of the elliptic curve version of the Schnorr identification scheme to provide mutual authentication between the BlackBerry Enterprise Server and device.
3. The BlackBerry Router opens an authenticated connection.

Closing a direct connection between a device and BlackBerry Router

If a user disconnects a BlackBerry device from a computer that hosts the BlackBerry Device Manager, closes the BlackBerry Device Manager, or disconnects the device from an enterprise Wi-Fi network, the device restores the connection to the BlackBerry Infrastructure over the wireless network automatically. The BlackBerry Enterprise Server and BlackBerry Router use the BlackBerry Router protocol to close the authenticated connection to the device. The BlackBerry Router protocol is designed to permit only an authenticated party to close the connection. The BlackBerry Router uses a single execution of the Schnorr identification scheme to authenticate the close command that the BlackBerry Enterprise Server sends to the BlackBerry Router.

Impersonation attacks that the BlackBerry Router protocol is designed to prevent

The BlackBerry Router protocol is designed to prevent a potentially malicious user from impersonating a BlackBerry device or a BlackBerry Enterprise Server.

To impersonate the device, the potentially malicious user sends messages to the BlackBerry Enterprise Server so that the BlackBerry Enterprise Server believes it is communicating with the device. To impersonate the BlackBerry Enterprise Server, the potentially malicious user sends messages to the device so that the device believes it is communicating with the BlackBerry Enterprise Server.

To perform either of these impersonation attacks, the potentially malicious user must send the device transport key value (also known as *s*) to the BlackBerry Enterprise Server or device, which requires the potentially malicious user to solve the discrete log problem to determine *s* or the hash of *s*.

How the BlackBerry Router protocol uses the Schnorr identification scheme to open an authenticated connection

The implementation of the Schnorr identification scheme in the BlackBerry Router protocol uses a group of large prime order, which is the additive group of elliptic curve points for a prime *p*.

The BlackBerry Router protocol is designed to perform the following actions:

- use the NIST recommended 521-bit elliptic curve group
- verify that the points supplied by the parties involved in the communication are members of the elliptic curve group
- verify that R_D does not equal R_B , to prevent the recovery of *h* by a potentially malicious user
- verify that *e* does not equal 0, to prevent the recovery of *h* by a potentially malicious user
- verify that R does not equal the point at infinity, to verify that R is a valid public key
- verify that *R* does not equal the point at infinity, to verify that *R* is a valid public key
- reset any corrupted data that it finds to a random value so that the BlackBerry Router protocol can proceed past the point that it detects corrupted data

Because the BlackBerry Router protocol can proceed past the point that it detects corrupted data, the BlackBerry Router protocol is unsuccessful at completion only. This measure is designed to prevent various timing attacks.

Data flow: Using the BlackBerry Router protocol to open an authenticated connection

1. The BlackBerry device and BlackBerry Enterprise Server hash the current device transport key using SHA-512.
2. The device performs the following actions:
   a selects a random value $r_{D,}$ where $1 < r_D < p - 1$ and calculates $R_D = r_D P$
   b sends R_D and a device transport key identifier (*KeyID*) to the BlackBerry Enterprise Server
3. The BlackBerry Router performs the following actions:
   a observes the data that the device sends and verifies that the value R_D is not the point at infinity
   b if R_D is the point at infinity, the BlackBerry Router configures R_D to a random value

c sends R_D and *KeyID* to the BlackBerry Enterprise Server

4. The BlackBerry Enterprise Server performs the following actions:
   a calculates that as R_D approaches the point at infinity, R_D is random
   b selects a random value r_B , where $1 < r_B < p - 1$ and calculates $R_B = r_B P$
   c if $R_D = R_B$, calculates another value of R_B
   d selects a random value e_D , where $1 < e_D < p - 1$
   e sends R_B , e_D , and *KeyID* to the device

5. The BlackBerry Router performs the following actions:
   a observes the data that the BlackBerry Enterprise Server sends
   b verifies that the value R_B is random when the value R_B approaches the point at infinity or when $R_D = R_B$
   c verifies that the value e_D is random when the value $e_D = 0$
   d sends R_B , e_D , and *KeyID* to the device

6. The device performs the following actions:
   a verifies that the value R_B is random when the value R_B approaches the point at infinity or when $R_D = R_B$
   b verifies that the value e_D is random when the value $e_D = 0$
   c calculates $y_D = h - e_D r_D \bmod p$
   d selects a random value e_B , where $1 < e_B < p - 1$
   e sends y_D and e_B to the BlackBerry Enterprise Server

7. The BlackBerry Router performs the following actions:
   a observes the data that the device sends
   b verifies that the value e_B is random if $e_B = 0$ or $e_B = e_D$
   c forwards y_D and e_B to the BlackBerry Enterprise Server

8. The BlackBerry Enterprise Server performs the following actions:
   a verifies that the value e_B is random when the value $e_D = e_B$
   b verifies that the value e_D is random when the value $e_D = 0$
   c computes $y_B = h - e_B r_B \pmod p$
   d sends y_B to the device

9. One of the following actions occurs:
   - The BlackBerry Enterprise Server and device open an authenticated connection to each other if the device accepts y_B.
   - The device does not accept the connection request, and the BlackBerry Enterprise Server and device do not open an authenticated connection to each other, if the device calculates the following:

$y_B P + e_B R_B \neq hP$

- The BlackBerry Router does not accept the connection request if the BlackBerry Router calculates the following:

  $y_B P + e_B R_B \neq y_D P + e_D R_D$

- The BlackBerry Enterprise Server does not accept the connection request if the BlackBerry Enterprise Server calculates the following:

  $y_D P + e_D R_D \neq hP$

- The BlackBerry Router stores R_D , R_B , $y_D P + e_D R_D$, e_D , and e_B if the device accepts y_B .

10. The BlackBerry Enterprise Server stores R_D , R_B , e_D , e_B , and h.
11. The BlackBerry Router overwrites y_B and y_D in memory with zeroes.
12. The BlackBerry Enterprise Server overwrites y_B , y_D , and r_B in memory with zeroes.
13. The device overwrites y_B , y_D , and r_D in memory with zeroes.

Data flow: Using the BlackBerry Router protocol to close an authenticated connection

1. The BlackBerry Enterprise Server performs the following actions:
   a selects a random value r_C , where $1 < r_c < p - 1$
   b calculates $R_C = r_C P$
   c calculates another R_C value if $R_C = R_B$, or $R_C = R_D$
   d sends the value R_C to the BlackBerry Router

2. The BlackBerry Router performs the following actions:
   a verifies that the value R_C is random when the value R_C approaches the point at infinity
   b verifies that the value R_C is random when the value $R_C = R_B$, or $R_C = R_D$
   c selects a random value e_C , where $1 < e_c < p - 1$
   d calculates another e_C value if $e_C = e_D$, or $e_c = e_B$
   e sends the value e_C to the BlackBerry Enterprise Server

3. The BlackBerry Enterprise Server performs the following actions:
   a verifies that the value e_C is random when the value $e_C = 0$
   b verifies that the value e_C is random when the value $e_C = e_B$, or $e_C = e_D$
   c calculates $y_C = h - e_C r_C \bmod p$
   d sends the value y_C to the BlackBerry Router

4. The BlackBerry Router performs one of the following actions:
   - The BlackBerry Router closes the authenticated connection to the BlackBerry device on behalf of the BlackBerry Enterprise Server if the BlackBerry Router accepts y_C.
   - The BlackBerry Router does not close the authenticated connection to the device if the BlackBerry Router calculates the following:

     $$y_C P + e_C R_C \neq y_D P + e_D R_D$$

Cryptosystem parameters that the BlackBerry Router protocol uses

The BlackBerry Router, BlackBerry Enterprise Server, and BlackBerry device are designed to share the following cryptosystem parameters when they use the BlackBerry Router protocol.

Parameter	Description
E(Fq)	This parameter represents the NIST approved 521-bit random elliptic curve over *Fq*, which has a cofactor of 1. The BlackBerry Router protocol does all math operations in the groups *E(Fq)* and Z_p.
Fq	This parameter represents a finite field of prime order *q*.
P	This parameter represents a point of *E* that generates a prime subgroup of *E(Fq)* of order *p*.
xR	This parameter represents the elliptic curve scalar multiplication, where *x* is the scalar and *R* is a point on *E(Fq)*.
s	This parameter represents the value of the device transport key.
h	This parameter represents the SHA-512 hash of *s*.

Best practice: Protecting plain text messages that a device sends over the wireless network

Plain text messages include SMS text messages, MMS messages, and PIN messages. A BlackBerry device can send SMS text messages and MMS messages over a wireless TCP/IP connection.

Best practice	Description
Prevent a user from sending, forwarding, or replying to specific types of message on the device.	Consider the following guidelines: • Prevent a user from forwarding or replying to a message using a BlackBerry Enterprise Server that did not deliver the original message. • Prevent a user from using an email account to forward or reply to a PIN message or reply to an email message with a PIN message. To apply this best practice, you can use the Disable Forwarding Between Services IT policy rule.
Prevent external connections to a device.	Consider preventing applications on a device from opening external connections (for example, to WAP, SMS, MMS, or other public gateways). To apply this best practice, you can use the Allow External Connections IT policy rule.
Require S/MIME encryption or PGP encryption for PIN messages.	Consider preventing a user from sending PIN messages that are not S/MIME encrypted or PGP encrypted if your organization uses a highly secure messaging solution such as the S/MIME Support Package for BlackBerry smartphones or the PGP Support Package for BlackBerry smartphones. To apply this best practice, you can use the Disable Peer-to-Peer Normal Send IT policy rule.
Prevent a device from using the global PIN encryption key.	Considering the following guidelines: • Limit the number of devices in your organization's environment that can receive BlackBerry Messenger messages and PIN messages that use the global PIN encryption key. • Limit the number of devices in your organization that can receive PIN messages that use the PIN encryption key that is specific to your organization, the global PIN encryption key, or both.

Best practice	Description
	To apply this best practice, you can use the Firewall Block Incoming Messages IT policy rule.
Require a user to verify whether the user wants to send a message.	Consider configuring the device so that the user must verify whether the user wants to send an email message, SMS text message, MMS message, or PIN message. To apply this best practice, you can use the Confirm on Send IT policy rule.
Turn off unsecured messaging on the device.	Consider turning off unsecured messaging to make sure that all communication for the device that starts in your organization travels through your organization's messaging environment. To turn off SMS text messaging, you can use the Allow SMS IT policy rule. To turn off MMS messaging, you can use the Disable MMS IT policy rule. To turn off PIN messaging, you can use the Allow Peer-to-Peer Messages IT policy rule. When you turn off PIN messaging, a user can receive PIN messages on the device but cannot send PIN messages from the device.

How the BlackBerry Enterprise Server protects connections between a device and the Internet or intranet

A user can use the BlackBerry Browser and BlackBerry Applications on a BlackBerry device to access the Internet and your organization's intranet. The BlackBerry Browser and BlackBerry Java Applications can accept and respond to push requests from push applications. The BlackBerry Browser and BlackBerry Java Applications use the BlackBerry MDS Connection Service to access the Internet and your organization's intranet.

To access data on the Internet or your organization's intranet, the BlackBerry MDS Connection Service uses HTTP, TCP/IP, and the BlackBerry MDS security protocol. The BlackBerry MDS security protocol is a Research In Motion proprietary protocol that is designed to protect messages that the device sends using the BlackBerry MDS Connection Service. The BlackBerry MDS Connection Service and device use BlackBerry transport layer encryption to help protect your organization's applications and the Internet data that a user receives on the device.

Protecting HTTP connections from a device to content servers and application servers using HTTPS

If a third-party application on a BlackBerry device can access servers on the Internet, you can configure the BlackBerry MDS Connection Service to use HTTPS to provide additional authentication and security for the connection. The device supports HTTPS in proxy mode using a proxy server or in direct mode using TLS.

If you configure HTTPS using a proxy server, the BlackBerry MDS Connection Service uses cipher suite components of Sun JSSE version 1.4.1 to open the connection for the device. Typically, HTTP connections open faster using a proxy server than TLS.

If you configure HTTPS using TLS, the BlackBerry MDS Connection Service uses the TLS and WTLS key establishment algorithms, symmetric algorithms, and hash algorithms that the RIM Cryptographic API supports to open the connection for the device. The device uses TLS to encrypt data that an application sends to content servers. The BlackBerry MDS Connection Service does not decrypt data that it sends over the wireless network. You can use TLS when only the end points of the transaction are trusted (for example, with banking services). A device that is running BlackBerry Device Software version 3.6.1 or later supports TLS for connections.

Warning messages for invalid certificates

If a BlackBerry device user visits a website that presents an invalid certificate, the BlackBerry device displays one of the following warning messages:

Warning message	Description
Domain Name Mismatch	The server uses a domain name that does not match any of the domain names in the server's certificate.
Expired Certificate	The certificate is expired.
Not Yet Valid	The certificate has not yet reached the date when it becomes valid.
Untrusted Certificate	The certificate cannot be trusted because there is a problem with the certificate chain or the certification authority.

Warning message	Description
Weak Crypto Algorithm	Your organization considers the algorithm that is used in the certificate chain to be weak.

Permitting TLS connections to websites that use invalid certificates

If a BlackBerry device user visits a website that presents an invalid certificate, the BlackBerry device displays a warning message to indicate that the security of the connection cannot be verified. The warning dialog box provides the user with the following options:

- Continue: the user should select this option if the user trusts the website. If the user selects Continue, the device adds the website to the Server Exceptions list in the TLS settings on the device. The device does not display a warning message for that web site again. The user can view or delete entries in the Server Exceptions list.
- Stop: the user should select this option if the user does not trust the website. If the user selects Stop, the device closes the connection between the device and the website.
- Details: the user should select this option if the user is not sure about whether to trust the website. If the user selects Details, the device shows information about the invalid certificate and permits the user to view the certificate.

When a website certificate changes

If the certificate for a website changes, the website is removed from the Server Exceptions list in the TLS settings on the BlackBerry device. A device does not display a notification that the website was removed from the Server Exceptions list. The next time that the BlackBerry device user visits the website after the website was removed from the list, if the new certificate that the website presents is invalid, the device displays a warning message indicating that the security of the connection cannot be verified. If the user trusts the website, the user must add the website to the Server Exceptions list again.

When IT policy rule changes affect TLS settings

If you change the values for any IT policy rules in the TLS Application policy group that affect TLS settings, any websites in the Server Exceptions list that are affected by the change remain in the Server Exceptions list. If a BlackBerry device user connects to a website and encounters a TLS warning that is restricted by an IT policy rule, the website is removed from the Server Exceptions list and the BlackBerry device displays a warning message indicating that the security of the connection cannot be verified. The warning dialog box presents the user with the following options:

- Stop: the user should select this option if the user wants to close the connection between the device and the website.
- Details: the user should select this option if the user wants to see more information about why the certificate is invalid. When the user selects Details, the device shows information about the invalid certificate and indicates that the policy does not permit the connection.

For more information about IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*.

How a device protects a connection to a WAP gateway

BlackBerry Device Software versions 3.2 SP1 and later supports WTLS, which is designed to provide additional security when a BlackBerry device connects to a WAP gateway. A device can connect to a WAP gateway to access services that are provided by your organization's wireless service provider or to access a web site. WTLS encrypts and decrypts information, authenticates users, and provides data integrity.

For more information about WAP gateways, see your organization’s wireless service provider.

What happens to data that is not delivered to a device

What happens to data that is not delivered because the connection between a BlackBerry Enterprise Server and the BlackBerry Infrastructure closes

Ten minutes after the connection between a BlackBerry Enterprise Server and the BlackBerry Infrastructure closes, the BlackBerry Infrastructure notifies the sender’s BlackBerry device and deletes the message that is not delivered. The wireless network can queue up to 5 undelivered messages for up to 7 days. If more than 5 undelivered messages exist in the queue, the BlackBerry Enterprise Server stores the messages in the BlackBerry Configuration Database. The BlackBerry Infrastructure does not store data to send to devices.

If the BlackBerry Infrastructure is not responding and the connection closes unexpectedly, the wireless network deletes the undelivered messages. The device does not receive the messages and it does not send acknowledgment packets to the

BlackBerry Enterprise Server. When the BlackBerry Infrastructure becomes available again, the BlackBerry Enterprise Server resends messages that it did not receive acknowledgment packets for.

What happens to data that is not delivered because a device is not available on the wireless network

When a user sends a message from a BlackBerry device, the BlackBerry Infrastructure might not be able to deliver the message to a device immediately if the device is not available on the wireless network. A device might not be available if it is outside a wireless coverage area or if the device is turned off.

If the BlackBerry Infrastructure cannot deliver a message after 10 minutes, the BlackBerry Infrastructure notifies the BlackBerry Enterprise Server and deletes the message. The BlackBerry Enterprise Server requests a notification message from the BlackBerry Infrastructure when the device becomes available over the wireless network. When the device becomes available over the wireless network, the BlackBerry Infrastructure notifies the BlackBerry Enterprise Server. The BlackBerry Enterprise Server sends the message to the device.

If the message is not delivered after 7 days, the BlackBerry Infrastructure notifies the sender's device that it cannot deliver the message.

Protecting communications in your organization's environment

11

How a BlackBerry Enterprise Server and the BlackBerry Infrastructure authenticate with each other

The BlackBerry Infrastructure and BlackBerry Enterprise Server must authenticate with each other before they can transfer data. The BlackBerry Enterprise Server uses SRP to authenticate with and connect to the BlackBerry Infrastructure.

SRP is a point-to-point protocol that runs over TCP/IP. The BlackBerry Enterprise Server uses SRP to contact the BlackBerry Infrastructure and open a connection. When the BlackBerry Enterprise Server and BlackBerry Infrastructure open a connection, they perform the following actions:

- authenticate with each other
- exchange configuration information
- send and receive data

The BlackBerry Enterprise Server and BlackBerry Infrastructure use the SRP authentication key when they authenticate with each other. The SRP authentication key is a 20-byte encryption key that the BlackBerry Enterprise Server and BlackBerry Infrastructure share.

The BlackBerry Enterprise Server sends only outgoing traffic to a BlackBerry device using an authenticated connection to the BlackBerry Infrastructure.

What happens when a BlackBerry Enterprise Server and the BlackBerry Infrastructure open an initial connection

After a BlackBerry Enterprise Server and the BlackBerry Infrastructure open an initial connection over the Internet, the BlackBerry Enterprise Server is designed to send a basic information packet to the BlackBerry Infrastructure immediately. A basic information packet includes version information, SRP identifiers, and other information that is required to open an SRP connection. Both the BlackBerry Enterprise Server and BlackBerry Infrastructure can recognize the basic information packet. The BlackBerry Enterprise Server and BlackBerry Infrastructure can use the basic information packet to configure the parameters of the SRP implementation.

The BlackBerry Infrastructure does not send basic information packets to the BlackBerry Enterprise Server until after the BlackBerry Enterprise Server sends a packet to the BlackBerry Infrastructure. This process permits the BlackBerry Infrastructure to be backward compatible with previous BlackBerry Enterprise Server versions, which close the SRP connection if they receive unrecognized basic information packets.

How the BlackBerry Enterprise Solution protects a TCP/IP connection between a BlackBerry Enterprise Server and the BlackBerry Infrastructure

After a BlackBerry Enterprise Server and the BlackBerry Infrastructure open an SRP connection, the BlackBerry Enterprise Server uses a persistent TCP/IP connection to send data to the BlackBerry Infrastructure. The BlackBerry Infrastructure uses wireless network protocols (for example, GSM or EDGE) to send data to the BlackBerry device. The TCP/IP connection between the BlackBerry Enterprise Server and BlackBerry Infrastructure is designed to be highly secure in the following ways:

- The BlackBerry Enterprise Server deletes data traffic that it receives from any source other than the messaging server, or from the device through the BlackBerry Infrastructure or BlackBerry Desktop Software.
- The BlackBerry Enterprise Server and device use BlackBerry transport layer encryption to encrypt the data that they send to each other. No intermediate point decrypts and encrypts the data again.
- No data traffic of any kind can occur between the BlackBerry Enterprise Server and either the wireless network or the device unless the BlackBerry Enterprise Server can decrypt the data using a valid device transport key. Only the BlackBerry Enterprise Server and device have the correct device transport key.

You must configure your organization’s firewall or proxy server to permit the BlackBerry Enterprise Server to start and maintain an outgoing connection to the BlackBerry Infrastructure over TCP port 3101.

Data flow: Authenticating a BlackBerry Enterprise Server with the BlackBerry Infrastructure

1. The BlackBerry Enterprise Server sends a data packet that contains its unique SRP identifier to the BlackBerry Infrastructure to claim the SRP identifier.
2. The BlackBerry Infrastructure sends a random challenge string to the BlackBerry Enterprise Server.
3. The BlackBerry Enterprise Server sends a challenge string to the BlackBerry Infrastructure.
4. The BlackBerry Infrastructure hashes the challenge string with the SRP authentication key using HMAC with the SHA-1 algorithm. The BlackBerry Infrastructure sends the resulting 20-byte value to the BlackBerry Enterprise Server as a challenge string.
5. The BlackBerry Enterprise Server hashes the challenge string with the SRP authentication key, and sends a challenge response to the BlackBerry Infrastructure.
6. The BlackBerry Infrastructure performs one of the following actions:

   - accepts the challenge response and sends a confirmation to the BlackBerry Enterprise Server to complete the authentication process and configure an authenticated SRP connection
   - rejects the challenge response

   If the BlackBerry Infrastructure rejects the challenge response, the authentication process is not successful. The BlackBerry Infrastructure and BlackBerry Enterprise Server close the SRP connection. If a BlackBerry Enterprise Server uses the same SRP authentication key and SRP identifier to connect to (and then disconnect from) the BlackBerry Infrastructure 5 times in 1 minute, the BlackBerry Infrastructure deactivates the SRP identifier to help prevent a potentially malicious user from using the SRP identifier to create conditions for a DoS attack.

How a BlackBerry Enterprise Server and messaging server protect a connection to each other

A BlackBerry Enterprise Server is designed to connect to the following messaging servers in a highly secure manner.

Messaging server	Description
IBM Domino	The BlackBerry Enterprise Server and the Domino server communicate using the Notes RPC protocol.

Messaging server	Description
	A user who activates a BlackBerry device when the device is connected to a computer can encrypt data that is in transit between the Domino server and a Notes Inbox. For more information, see the online help for Domino.
Microsoft Exchange	The BlackBerry Enterprise Server and Microsoft Exchange Server can communicate using Microsoft Exchange Web Services or the Microsoft Exchange Server RPC protocol over a MAPI connection. When the BlackBerry Enterprise Server and Microsoft Exchange Server communicate using Microsoft Exchange Web Services they use an SSL connection. A user can use 128-bit encryption to encrypt RPC communication over the MAPI connection between the Microsoft Exchange server and Microsoft Outlook. For more information about turning on encryption, see the documentation for Microsoft Exchange .
Novell GroupWise	The BlackBerry Enterprise Server is designed to use a trusted application key to open a connection to the Novell GroupWise server. To generate the trusted application key, an administrator of Novell GroupWise runs the trusted application key generator, specifies the location of the primary domain of Novell GroupWise, and specifies the application name that the BlackBerry Enterprise Server can use to connect to the Novell GroupWise server. The trusted application key is a 64-byte ASCII string. The BlackBerry Enterprise Server connects to a user's mailbox in a highly secure manner using the trusted application key. The Novell GroupWise server verifies the trusted application key and permits the BlackBerry Enterprise Server to open a connection to the Novell GroupWise database for the user.

How the BlackBerry Enterprise Server components and the BlackBerry MVS protect communication

BlackBerry Enterprise Server components and the BlackBerry Mobile Voice System use the BlackBerry inter-process protocol to help protect the data that the components send to each other. The BlackBerry inter-process protocol uses a communication password to generate a session key that encrypts the data that the components send to each other. The BlackBerry Collaboration Service, BlackBerry MDS Connection Service, BlackBerry Policy Service, BlackBerry

Synchronization Service, and BlackBerry MVS share a communication password. The BlackBerry Messaging Agent and BlackBerry Dispatcher share a different communication password. The communication passwords are designed to prevent a potentially malicious user from viewing data that the BlackBerry Enterprise Server components and the BlackBerry MVS send to each other.

When a BlackBerry Enterprise Server component or the BlackBerry MVS opens a connection to the BlackBerry Dispatcher, the BlackBerry inter-process protocol is designed to use SPEKE to generate the session key. The key generation process uses the communication password of the BlackBerry Enterprise Server component or BlackBerry MVS and generates an AES-256 encryption key, which is the session key. The BlackBerry Enterprise Server components and BlackBerry MVS use the session key to encrypt the data that the BlackBerry Enterprise Server components and BlackBerry MVS sends to other BlackBerry Enterprise Server components that share the same communication password.

How the BlackBerry Desktop Manager protects communication using the BlackBerry inter-process protocol

The application loader tool of the BlackBerry Desktop Manager or the Roxio Media Manager for BlackBerry smartphones can prompt BlackBerry Desktop Manager version 4.2 or later for the BlackBerry device password.

To protect the BlackBerry device password, when the application loader tool or Roxio Media Manager for BlackBerry smartphones connects to the BlackBerry Desktop Manager, the BlackBerry Desktop Manager uses the BlackBerry inter-process protocol.

The application loader tool and Roxio Media Manager for BlackBerry smartphones share a communication password with the BlackBerry Desktop Manager. The BlackBerry inter-process protocol is designed to use the communication password to protect any communication between the BlackBerry Desktop Manager and the application loader tool or Roxio Media Manager for BlackBerry smartphones.

Data flow: Authenticating the application loader tool or Roxio Media Manager with the BlackBerry Desktop Software using the BlackBerry inter-process protocol

1. The application loader tool of the BlackBerry Desktop Software or Roxio Media Manager opens a connection to BlackBerry Desktop Software version 4.2 or later.
2. The BlackBerry Desktop Software implementation of the BlackBerry inter-process protocol performs the following actions:

a uses a shared secret password (also known as the communication password) and the ECDH protocol with a 521-bit curve to create a device transport key

b uses the device transport key to create two encryption keys and two HMAC-SHA-256 keys

c uses one encryption key and one HMAC key to encrypt and authenticate data that BlackBerry Desktop Software version 4.2 or later sends over the communication channel to the BlackBerry Enterprise Solution components that share the communication password

The BlackBerry inter-process protocol uses one encryption key and one HMAC key to encrypt and authenticate data that BlackBerry Desktop Software version 4.2 receives over the communication channel from the application loader tool or Roxio Media Manager.

How the BlackBerry Collaboration Service connects to an instant messaging server and collaboration clients on devices

The BlackBerry Collaboration Service is designed to connect to an instant messaging server and the collaboration clients on BlackBerry devices. If your organization's instant messaging server is Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007, the BlackBerry Collaboration Service connects to the Microsoft Office Communicator Web Access server using HTTPS or HTTP.

Protecting your organization's resources when using BlackBerry MDS Connection Service integrated authentication

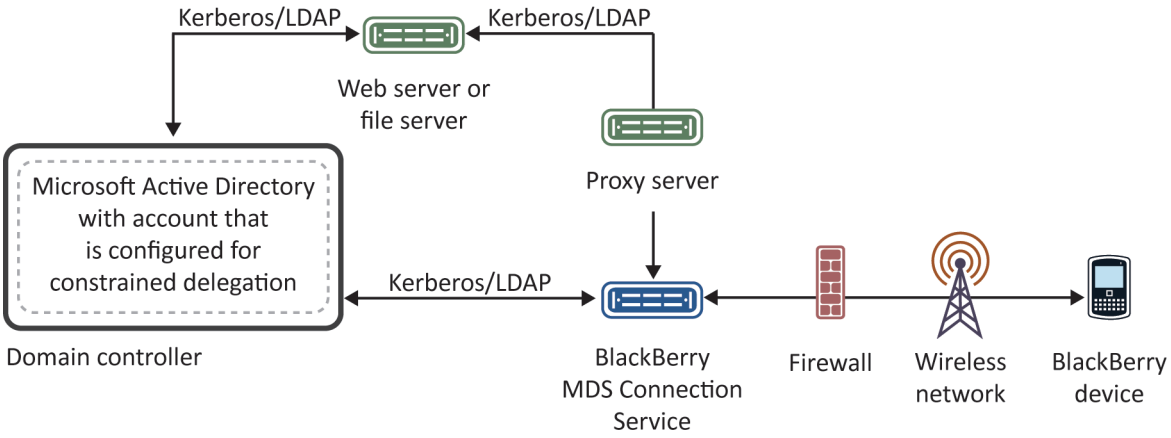
You can configure the BlackBerry MDS Connection Service to support Integrated Windows authentication so that BlackBerry device users can access the intranet or shared files from the BlackBerry Browser or the Files application on devices. By default, if you configure the BlackBerry MDS Connection Service and users access the intranet or a shared file, the users must authenticate with your organization's domain controller by providing their Microsoft Active Directory account passwords. In BlackBerry Enterprise Server 5.0 SP2, you can configure the BlackBerry MDS Connection Service so that users are not required to type a password each time they want to access a resource.

If you configure the BlackBerry MDS Connection Service to support Integrated Windows authentication, the BlackBerry MDS Connection Service uses the Kerberos protocol and constrained delegation to help protect your organization's

environment and authenticate and authorize users. The Kerberos protocol is designed to permit the BlackBerry MDS Connection Service to verify user accounts in Microsoft Active Directory. Constrained delegation is designed to limit the resources that the BlackBerry MDS Connection Service can provide authenticated users access to.

If you want to configure both BlackBerry Administration Service single sign-on and BlackBerry MDS Connection Service integrated authentication, you should configure separate Microsoft Active Directory accounts for the BlackBerry Administration Service and BlackBerry MDS Connection Service.

Architecture: BlackBerry MDS Connection Service integrated authentication



Component	Description
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service permits BlackBerry device users to access web content, the Internet, or your organization's intranet. It also permits applications on devices to connect to your organization's application servers or content servers for application data and updates.
domain controller	A domain controller is a server that authenticates and authorizes Windows users and Windows servers with a Windows domain.
Microsoft Active Directory	Microsoft Active Directory is an LDAP directory that stores user information.

How the BlackBerry MDS Connection Service uses Kerberos to help protect your organization's resources

BlackBerry MDS Connection Service integrated authentication is designed to use the Kerberos protocol and constrained delegation to authenticate BlackBerry device users in your organization's network in a highly secure manner. BlackBerry MDS Connection Service authenticates with Microsoft Active Directory on behalf of users, verify the users' identities, and retrieve the resource on behalf of the users.

The BlackBerry MDS Connection Service hosts a Kerberos service that permits it to verify users. To support BlackBerry MDS Connection Service integrated authentication, you must configure Microsoft Active Directory accounts in the Microsoft Active Directory domains that include the resources and configure constrained delegation for the Microsoft Active Directory accounts. To configure constrained delegation, you must configure the Microsoft Active Directory accounts to trust only the Kerberos service that is hosted by the BlackBerry MDS Connection Service.

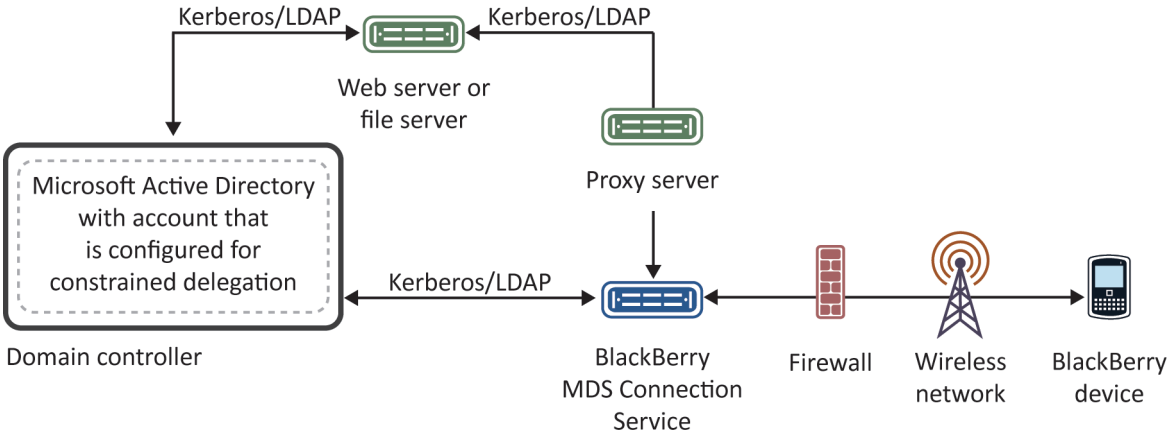
When the BlackBerry MDS Connection Service starts, it authenticates with the Microsoft Active Directory domain using the Microsoft Active Directory account. The domain controller issues the Kerberos keys and Kerberos service ticket to the Kerberos service. The Kerberos keys permit the BlackBerry MDS Connection Service to verify the Kerberos service tickets for users.

Identifying the resources that users can access using BlackBerry MDS Connection Service integrated authentication

If you configure the BlackBerry MDS Connection Service to support the Kerberos protocol and constrained delegation, you must use the BlackBerry Administration Service to specify the pull rules that identify the shared files or intranet resources that you want to permit Integrated Windows authentication for. You must assign the pull rules to groups or user accounts so that the BlackBerry MDS Connection Service can determine which user accounts to apply the pull rules to. Pull rules permit you to specify the shared files or intranet resources in your organization's network that you want users to access from BlackBerry devices and the authentication method that you want users to use to access the shared files or Intranet resources.

For information about configuring pull rules, see the *BlackBerry Enterprise Server Administration Guide*.

Data flow: Retrieving a resource when using BlackBerry MDS Connection Service integrated authentication



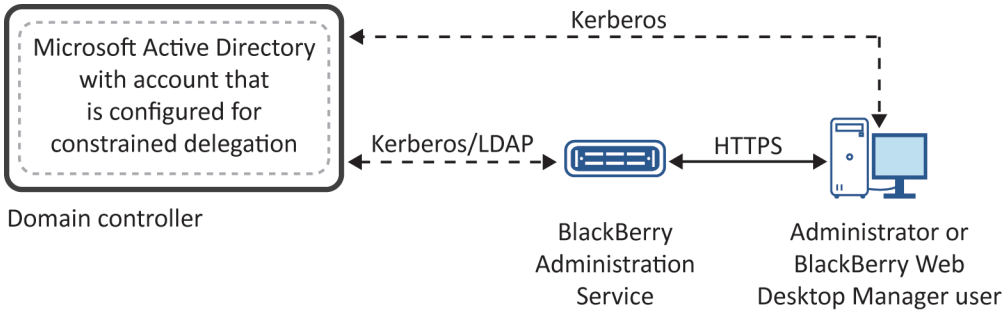
1. The BlackBerry device user navigates to a resource on your organization's intranet or on a file share (for example, a web page or shared file) using the BlackBerry Browser or Files application on the BlackBerry device.
2. The device encrypts and compresses an HTTP request for the resource and sends the encrypted HTTP request to the BlackBerry Router using BlackBerry transport layer encryption.
3. The BlackBerry Router forwards the encrypted HTTP request to the BlackBerry Dispatcher.
4. The BlackBerry Dispatcher decrypts and decompresses the HTTP request and forwards the request to the BlackBerry MDS Connection Service.
5. The BlackBerry MDS Connection Service performs the following actions:
   - verifies whether the resource is located in a Microsoft Active Directory domain that is configured for Integrated Windows authentication
   - checks the pull rules assigned to the user accounts and verifies that the user must use Integrated Windows authentication to access the resource
   - connects to the Microsoft Active Directory using its Microsoft Active Directory account that is configured for constrained delegation
   - retrieves the Microsoft Active Directory user name for the user from Microsoft Active Directory
   - retrieves the Kerberos service ticket for the user from Microsoft Active Directory using the S4U2proxy extension
   - encodes the service ticket using Base-64 encoding and adds the service ticket to the header of the HTTP request
   - resends the request for the resource to the web server or file system that hosts the resource
6. The web server or file system returns the resource to BlackBerry MDS Connection Service.
7. The BlackBerry MDS Connection Service forwards the resource to the BlackBerry Dispatcher.
8. The BlackBerry Dispatcher encrypts and compresses the resource and splits it into packages and sends the packages to the BlackBerry Router.
9. The BlackBerry Router sends the packages to the device using BlackBerry transport layer encryption.
10. The device decrypts and decompresses the packages and displays the resource to the user.

Protecting your organization's resources when you configure BlackBerry Administration Service single sign-on

You can configure the BlackBerry Administration Service so that administrators or BlackBerry Web Desktop Manager users must log in to the BlackBerry Administration Service console or BlackBerry Web Desktop Manager using Microsoft Active Directory authentication. If you configure the BlackBerry Administration Service to support Microsoft Active Directory authentication in BlackBerry Enterprise Server 5.0 SP2, you can also configure single sign-on so that administrators or users can access the BlackBerry Administration Service console or BlackBerry Web Desktop Manager directly without logging in.

If you configure single sign-on, the BlackBerry Administration Service uses the Kerberos protocol and constrained delegation to help protect your organization's environment and authenticate and authorize administrators and users. The Kerberos protocol is designed to permit the BlackBerry Administration Service to verify administrator accounts and user accounts in Microsoft Active Directory. Constrained delegation is designed to limit the resources that the BlackBerry Administration Service can provide authenticated administrators and users access to.

Architecture: BlackBerry Administration Service single sign-on



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Domain, which includes BlackBerry Enterprise Server components, user accounts, and features for BlackBerry device administration.
domain controller	A domain controller is a server that authenticates and authorizes Windows users and Windows servers with a Windows domain.
Microsoft Active Directory	Microsoft Active Directory is an LDAP directory that stores user information.

How BlackBerry Administration Service single sign-on uses Kerberos to help protect your organization's resources

BlackBerry Administration Service single sign-on implements Kerberos authentication which permits the BlackBerry Administration Service to authenticate administrators and BlackBerry Web Desktop Manager users in your organization's network in a highly secure manner.

The BlackBerry Administration Service includes two Kerberos services that it uses to authenticate with browsers. The BlackBerry Administration Service application server and BlackBerry Administration Service web server host the Kerberos services. The BlackBerry Administration Service requires two Kerberos services so that it can authenticate the web layer and application layer. The Kerberos service that the BlackBerry Administration Service web server hosts verifies requests from browsers to access the web layer. The Kerberos service that the BlackBerry Administration Service application server hosts verifies requests from the BlackBerry Administration Service web server to access the application layer.

The Kerberos services are identified using SPNs that you create and assign to a Microsoft Active Directory account. You must create the Microsoft Active Directory account as a Kerberos service account in the Microsoft Active Directory domain that includes the BlackBerry Administration Service and configure constrained delegation for the Microsoft Active Directory account. You must configure the Microsoft Active Directory account to trust only the Kerberos service that the BlackBerry Administration Service application server hosts for constrained delegation and only when the BlackBerry Administration Service application service is using Kerberos.

If your organization's environment includes multiple Microsoft Active Directory account forests, you must configure a Microsoft Active Directory account for each account forest. However, you do not need to configure constrained delegation for the Microsoft Active Directory accounts that you configure in the account forests.

How the BlackBerry Administration Service completes Kerberos authentication

When the BlackBerry Administration Service starts, it authenticates with the Microsoft Active Directory domain using the Microsoft Active Directory account. The domain controller issues the Kerberos keys and Kerberos service ticket for the two

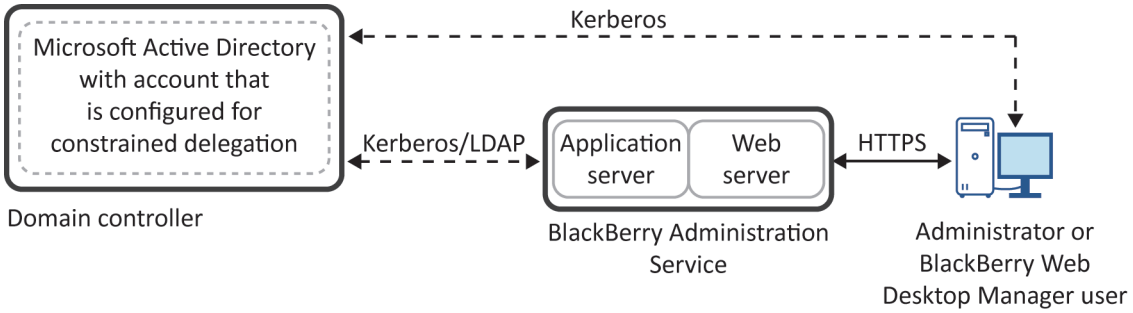
Kerberos services. The Kerberos keys permit the BlackBerry Administration Service to verify the Kerberos service tickets that browsers send during single sign-on.

Browsers that support Integrated Windows authentication can obtain the Kerberos service ticket automatically for the BlackBerry Administration Service when administrators or users browse to the BlackBerry Administration Service console or BlackBerry Web Desktop Manager.

The Kerberos service that the BlackBerry Administration Service web server hosts uses its Kerberos keys to verify the Kerberos service tickets that browsers send when they request access to the BlackBerry Administration Service console or BlackBerry Web Desktop Manager. If the Kerberos service tickets are valid, the BlackBerry Administration Service web server delegates the request to the BlackBerry Administration Service application server.

To delegate the request, the BlackBerry Administration Service web server creates a service ticket using its identity for the Kerberos service that the BlackBerry Administration Service application server hosts. When the Kerberos service that the BlackBerry Administration Service application server hosts verifies the service ticket, the BlackBerry Administration Service completes the Kerberos authentication process for the administrators or users and the administrators or users can view the BlackBerry Administration Service console home page or BlackBerry Web Desktop Manager home page.

Data flow: Accessing the BlackBerry Administration Service console and BlackBerry Web Desktop Manager when you configure BlackBerry Administration Service single sign-on



1. An administrator or a BlackBerry Web Desktop Manager user uses a browser to navigate to the BlackBerry Administration Service web page (https://<*BAS_pool_FQDN*>/webconsole/login) or BlackBerry Web Desktop Manager web page (https://<*BAS_pool_FQDN*>/webdesktop/login).
2. The BlackBerry Administration Service web server sends an HTTP Negotiate request to the browser to start single sign-on authentication.

   For more information about the HTTP Negotiate request, see http://msdn.microsoft.com/en-us/library/ms995330.aspx.

3. The browser retrieves the TGT of the administrator or user from the ticket cache on the computer that the administrator or user is using.

   The browser uses the TGT to request the service ticket for the BlackBerry Administration Service web server (which is named HTTP/<*BAS_pool_FQDN*>) from the domain controller.

4. The domain controller provides the browser with the service ticket for the BlackBerry Administration Service web server.
5. The browser sends the service ticket to the BlackBerry Administration Service web server in response to the HTTP-Negotiate request.
6. The BlackBerry Administration Service web server performs the following actions:

   - It validates the service ticket using the Kerberos key that it received from the domain controller when the BlackBerry Administration Service services started.
   - It requests a service ticket for the BlackBerry Administration Service application server (which is named BASPLUGIN111/<*BAS_pool_FQDN*>) on behalf of the user.

7. The domain controller provides the BlackBerry Administration Service web server with the service ticket for the BlackBerry Administration Service application server.
8. The BlackBerry Administration Service web server sends the service ticket to the BlackBerry Administration Service application server.
9. The BlackBerry Administration Service application server performs the following actions:

   - It validates the service ticket using the Kerberos key that it received from the domain controller when the BlackBerry Administration Service services started. If the service ticket is valid, the administrator or user is authenticated successfully with the BlackBerry Administration Service using Kerberos.
   - It checks if the administrator or user is a BlackBerry device user or a BlackBerry Administration Service administrator.
   - It checks the role of the administrator or user and assigns the administrator or user the permissions that are associated with the role.
   - It sends a security session to the BlackBerry Administration Service web server for the administrator or user.

10. The BlackBerry Administration Service web server redirects the administrator or user to the BlackBerry Administration Service console home page or BlackBerry Web Desktop Manager home page.

Activating a device

12

When a user activates a BlackBerry device, the BlackBerry Enterprise Solution authenticates the user and associates the device with a BlackBerry Enterprise Server. During the activation process, the BlackBerry Enterprise Solution generates a device transport key.

A user can activate the device over the wireless network, when the device is connected to a computer that is running the BlackBerry Desktop Software, or when the device is connected to a computer and the user is logged in to the BlackBerry Web Desktop Manager or BlackBerry Administration Service. The user must have a valid email address so that the user can activate the device and register the device with the wireless network.

Activating a device over the wireless network

If a user activates a BlackBerry device over the wireless network, the user must authenticate with the device using an activation password that you provide. You can create an activation password using the BlackBerry Administration Service and communicate it to the user. You can also use IT policy rules to configure password requirements (such as duration, length, and strength), to specify password patterns, and to prevent specific passwords. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

The device uses the activation password to generate the device transport key. The device transport key authenticates the user and is designed to secure communication between the BlackBerry Enterprise Server and device.

An activation password has the following characteristics:

- applies to the user's email account
- is not valid after five unsuccessful attempts to activate the device
- expires if the user does not activate the device within the default period of time (48 hours), or a period of up to 720 hours that you can specify when you create the activation password

After the user activates the device, the BlackBerry Enterprise Server deletes the activation password. The user cannot use the same activation password to activate other devices.

Data flow: Activating a device over the wireless network

1. A user opens the activation application on the BlackBerry device, and types the appropriate email address and activation password.
2. The device sends an activation request to the BlackBerry Infrastructure using standard BlackBerry protocols. The BlackBerry Infrastructure uses SMTP to send an activation message to the user's email account. The activation message contains routing information for the device and public keys.
3. The BlackBerry Enterprise Server sends an activation response to the device. The activation response contains routing information for the BlackBerry Enterprise Server and the long-term public keys of the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server and device use the initial key establishment protocol to generate a device transport key and verify it. If the BlackBerry Enterprise Server and device mutually verify the device transport key, the activation process proceeds. The BlackBerry Enterprise Server and device use the device transport key to encrypt further communication between each other without sending the device transport key over the wireless network.
5. The BlackBerry Enterprise Server performs the following actions:
    - sends the appropriate service books to the device so that the user can send messages from and receive messages on the device
    - sends data (such as calendar entries, contacts, tasks, memos, and device options) to the device, if you turn on wireless organizer data synchronization and wireless backup

For more information about the activation process, see the *BlackBerry Wireless Enterprise Activation Technical Overview*.

Managing certificates on a device

13

Purpose of certificates on a device

A certificate is a digital document that binds the identity and public key of a certificate subject. Each certificate has a corresponding private key that is stored separately. A certification authority signs the certificate to verify that it can be trusted.

A BlackBerry device can use certificates to:

- Authenticate using SSL when it connects to web pages that use HTTPS
- Encrypt and sign email messages and PIN messages using S/MIME encryption
- Authenticate with an enterprise Wi-Fi network

Importing certificates onto a device

To permit a BlackBerry device to use certificates, you or a BlackBerry device user must import the certificates into the key store database in application storage. To import certificates, you or the user can use one or more of the following methods:

- Download certificates from the user's computer using the certificate synchronization tool in BlackBerry Desktop Software
- Enroll certificates over the wireless network
- Copy certificates from a media card or smart card
- Import certificates from an email attachment

To enroll certificates over the wireless network or copy them from a media card or smart card, you must use a device that is running BlackBerry Device Software 5.0 or later.

After you or the user imports the certificates, the device adds the certificates to the certificate list on the device.

For more information about how to import certificates, see the *BlackBerry Enterprise Server Administration Guide* and the user guide for the device.

Configuring BlackBerry devices to enroll certificates over the wireless network

You can configure the BlackBerry Enterprise Server to permit BlackBerry devices to enroll certificates that the devices can use with any PKI-enabled application or process. You can permit devices to enroll the certificates instead of instructing users to send the certificates to themselves in an email message or use the certificate synchronization tool in the BlackBerry Desktop Software. When you configure the BlackBerry Enterprise Server to permit devices to enroll certificates, you can control how users request certificates and which certification authority issues the certificates.

For example, you might want Wi-Fi enabled BlackBerry devices to enroll certificates so that they can authenticate to an enterprise Wi-Fi network.

You can enroll certificates from one of the following certification authorities:

- RSA certification authority
- Microsoft standalone certification authority
- Microsoft enterprise certification authority

During the enrollment process, the BlackBerry MDS Connection Service can verify the certificate if the certificate includes an email address in the subject DN. The BlackBerry MDS Connection Service verifies the certificate by checking if the email address in the subject DN of the certificate matches the email address that is assigned to the device. For more information about the enrollment process, see the *BlackBerry Enterprise Solution Security Technical Overview*.

You can make the certificate enrollment process required so that devices automatically start the certificate enrollment process after the devices receive the updated IT policy from the BlackBerry Enterprise Server. If you do not make the certificate enrollment process required, you must instruct users to start the CA Profile Manager on the devices manually.

Managing an enrolled certificate

After a BlackBerry device enrolls a certificate, the CA Profile Manager monitors the certificate's expiry date and revocation status. When the expiry date approaches or the certification authority revokes the certificate, the CA Profile Manager generates a new public-private key pair, and starts the certificate enrollment process for a new certificate.

The certificate enrollment process can also start again if you change the following IT policy rules and resend the IT policy:

- Certificate Authority Profile Name
- Certificate Authority Type
- Certificate Authority Host
- Common Name Components

- Custom Microsoft Certificate Authority Certificate Template
- Distinguished Name Components
- Key Algorithm
- Key Length
- Microsoft Certificate Authority Certificate Template
- RSA Certificate Authority Certificate ID
- RSA Jurisdiction ID

A certificate enrollment process does not delete the existing certificate from the device key store or notify the certification authority that the certificate is no longer in use. The BlackBerry Enterprise Server deletes the existing certificate from the BlackBerry Configuration Database when the certificate enrollment process starts for a new certificate.

Also, if a certificate is expired or revoked, you or a BlackBerry device user can update the certificates on the device using the certificate synchronization tool in the BlackBerry Desktop Software or by copying an updated certificate from a media card or smart card.

For more information about deleting or revoking certificates, see the user guide for the device.

Determining the status of certificates using a CRL or OCSP

To determine the status of a certificate, you can configure the BlackBerry MDS Connection Service to access CRL servers and OCSP servers on behalf of a BlackBerry device. The BlackBerry MDS Connection Service can retrieve the status of the certificate and provide the status to the device.

For more information about configuring the CRL servers and OCSP servers that the BlackBerry MDS Connection Service uses to retrieve the status of certificates, see the *BlackBerry Enterprise Server Administration Guide*. For more information about certificate status indicators, see the user guide for the device.

Data flow: Enrolling a certificate when the certification authority approves certificate requests automatically

After a BlackBerry device receives an IT policy that includes a certification authority profile, the enrollment process can start automatically, or you can instruct a user to start it. This process flow assumes that the certification authority in your organization's environment is a Microsoft enterprise certification authority.

1. The CA Profile Manager on the device generates the key pair for the certificate.
2. The BlackBerry MDS Connection Service authenticates the user.
3. The device requests the user's distinguished name from the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends the distinguished name to the device.
5. The device encrypts the key pair, and stores the key pair, distinguished name, and profile ID for the certification authority in the persistent store in flash memory.
6. The CA Profile Manager creates the PKCS #10 certificate request, and signs it with the private key.
7. The device sends the certificate request, profile ID for the certification authority, and Windows login information to the BlackBerry MDS Connection Service.
8. The BlackBerry MDS Connection Service performs one of the following actions:
   - sends the certificate chain to the BlackBerry Enterprise Server if the certificate chain is in the BlackBerry MDS Connection Service cache
   - retrieves the certificate chain from the certification authority and sends it to the BlackBerry Enterprise Server if the certificate chain is not in the BlackBerry MDS Connection Service cache
9. The BlackBerry Enterprise Server sends the certificate chain to the device.
10. The BlackBerry MDS Connection Service sends a status update to the device and sends the certificate request to the certification authority that is associated with the profile ID.
11. The certification authority issues the certificate, publishes it to the LDAP server, and notifies the BlackBerry MDS Connection Service that the certificate is available.
12. The BlackBerry MDS Connection Service performs the following actions:
    a. retrieves the certificate from the LDAP server that the certification authority publishes the certificate to
    b. sends the certificate to the BlackBerry Enterprise Server
13. The BlackBerry Enterprise Server performs the following actions:

a verifies the certificate by checking whether the public key matches the public key that is stored in the BlackBerry Configuration Database

b sends the certificate to the device over the wireless network

14. The device adds the certificate and private key to the key store.

Data flow: Enrolling a certificate when a certification authority administrator approves certificate requests

After a BlackBerry device receives an IT policy that includes a certification authority profile, the enrollment process can start automatically or you can instruct a user to start it. This process flow assumes that the certification authority in your organization's environment is a Microsoft enterprise certification authority.

1. The CA Profile Manager on the device generates the key pair for the certificate.
2. The BlackBerry MDS Connection Service authenticates the user.
3. The device requests the user's distinguished name from the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends the distinguished name to the device.
5. The device encrypts the key pair, and stores the key pair, distinguished name, and profile ID for the certification authority in the persistent store in flash memory.
6. The CA Profile Manager creates the PKCS #10 certificate request and signs it with the private key.
7. The device sends the certificate request, profile ID for the certification authority, and Windows login information to the BlackBerry MDS Connection Service.
8. The BlackBerry MDS Connection Service performs one of the following actions:
   - sends the certificate chain to the BlackBerry Enterprise Server if the certificate chain is in the BlackBerry MDS Connection Service cache
   - retrieves the certificate chain from the certification authority and sends it to the BlackBerry Enterprise Server if the certificate chain is not in the BlackBerry MDS Connection Service cache
9. The BlackBerry Enterprise Server sends the certificate chain to the device.
10. The BlackBerry MDS Connection Service sends a status update to the device and sends the certification request to the certification authority that is associated with the profile ID.
11. The certification authority performs the following actions:

    a waits for the certification authority administrator to approve the certificate request

b after the certification authority administrator approves the certificate request, issues the certificate, and sends the certificate to the user in an email message

12. The BlackBerry MDS Connection Service performs the following actions:
    a polls the user's mailbox on the messaging server, at specified intervals, for the certificate
    b sends the certificate to the BlackBerry Enterprise Server after the BlackBerry MDS Connection Service retrieves the certificate
13. The BlackBerry Enterprise Server performs the following actions:
    a verifies the certificate by checking whether the public key matches the public key that is stored in the BlackBerry Configuration Database
    b sends the certificate to the device over the wireless network
14. The device adds the certificate and private key to the key store.

Data flow: Enrolling a certificate using an RSA certification authority

After a BlackBerry device receives an IT policy that includes a certification authority profile, the enrollment process can start automatically or you can instruct a user to start it.

1. The CA Profile Manager on the device generates the key pair for the certificate.
2. The device requests the user's distinguished name from the BlackBerry Enterprise Server.
3. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends the distinguished name to the device.
4. The device encrypts the key pair, and stores the key pair, distinguished name, and profile ID for the certification authority in the persistent store in flash memory.
5. The CA Profile Manager creates the PKCS #10 certificate request and signs it with the private key.
6. The device sends the certificate request and the name of the certification authority profile to the BlackBerry MDS Connection Service.
7. The BlackBerry MDS Connection Service performs one of the following actions:
    - sends the certificate chain to the BlackBerry Enterprise Server if the certificate chain is in the BlackBerry MDS Connection Service cache
    - retrieves the certificate chain from the certification authority and sends it to the BlackBerry Enterprise Server if the certificate chain is not in the BlackBerry MDS Connection Service cache
8. The BlackBerry Enterprise Server sends the certificate chain to the device.

9. The BlackBerry MDS Connection Service sends a status update to the device and sends the certificate request to the certification authority that is associated with the name of the certification authority profile.
10. The certification authority performs the following actions:
    a waits for the certification authority administrator to approve the certificate request
    b after the certification authority administrator approves the certificate request, issues the certificate, and sends the URL for the certificate in an email message to the user
11. The BlackBerry Messaging Agent receives the email message and extracts the issue ID of the message from the URL and stores it in the BlackBerry Configuration Database.
12. The BlackBerry MDS Connection Service performs the following actions:
    a polls the BlackBerry Configuration Database every 5 minutes for the issue ID of the message, reconstructs the URL, and sends the URL to the certification authority to retrieve the certificate
    b sends the certificate to the BlackBerry Enterprise Server after retrieving the certificate
13. The BlackBerry Enterprise Server perfoms the following actions:
    a verifies the certificate by checking whether the public key matches the public key that is stored in the BlackBerry Configuration Database
    b sends the certificate to the device over the wireless network
14. The device adds the certificate and private key to the key store.

Protecting BlackBerry Device Software updates

14

Protecting BlackBerry Device Software updates over the wireless network

You can update the BlackBerry Device Software on a BlackBerry device over the wireless network. You can use the BlackBerry Administration Service to search for updates that match the device and wireless service provider, and send the updates. You can also permit your organization's wireless service provider to send the BlackBerry Device Software updates.

The BlackBerry Enterprise Solution protects the BlackBerry Device Software updates using encryption, IT policies, content protection, and battery power requirements.

For more information about BlackBerry Device Software updates, see the *BlackBerry Device Software Update Guide*.

How the BlackBerry Enterprise Solution protects BlackBerry Device Software updates over the wireless network using encryption

The BlackBerry Enterprise Server, BlackBerry Infrastructure, BlackBerry Provisioning System administration web site, and BlackBerry device protect data for BlackBerry Device Software updates over the wireless network. You can use the BlackBerry Provisioning System administration web site when you want to permit your organization’s wireless service provider to update the BlackBerry Device Software.

The BlackBerry Enterprise Server and device encrypt all data that they send between each other, including BlackBerry Device Software updates, using BlackBerry transport layer encryption.

The device validates the digital signatures of the following information to verify integrity:

- control messages that the device receives from the BlackBerry Infrastructure or BlackBerry Provisioning System administration web site
- BlackBerry Device Software update instructions that the device requests and receives from the BlackBerry Infrastructure or BlackBerry Provisioning System administration web site

How the BlackBerry Enterprise Solution protects BlackBerry Device Software updates over the wireless network using IT policies and content protection

The default values for the Default IT policy determine that only the BlackBerry Enterprise Server can send available updates and request a BlackBerry device to update the BlackBerry Device Software. A wireless service provider cannot send available BlackBerry Device Software updates to the device unless you change the value for the Allow Non Enterprise Upgrade IT policy rule to Yes.

When you or a user turns on the content protection feature on a device, the device protects user data in the following ways:

- requires the user to type the device password before the BlackBerry Device Software update process can back up or restore user data
- requires the device to encrypt stored user data during the BlackBerry Device Software update process

Battery power requirements for BlackBerry Device Software updates over the wireless network

The battery power level on a BlackBerry device must be 50% or greater for the BlackBerry device to retrieve an update package over the wireless network. If the battery power level is below the minimum requirement, the update process suspends. The BlackBerry device prompts the user to recharge the battery and start the BlackBerry Device Software update process again. If the battery power level returns to 50%, the BlackBerry device resumes retrieving the update package from the BlackBerry Infrastructure.

The battery power requirement is designed to protect the BlackBerry device against attacks from a potentially malicious user who might try to take advantage of low battery power during a BlackBerry Device Software update.

Data flow: Preparing to send a BlackBerry Device Software update over the wireless network

Before the BlackBerry Infrastructure sends a BlackBerry Device Software update to a BlackBerry device, the BlackBerry Infrastructure performs the following actions:

1. generates an ECDSA key periodically using ECC over a 521-bit curve
2. signs the ECDSA key using a stored root certificate
3. signs the BlackBerry Device Software update that it sends to the BlackBerry device using the digitally signed ECDSA key

How a device validates a BlackBerry Device Software update over the wireless network

When a BlackBerry device receives a BlackBerry Device Software update from the BlackBerry Infrastructure, it verifies that the ECDSA key uses a public key that is shared by all devices that support BlackBerry Device Software updates over the wireless network. The device verifies the digital signature on the ECDSA key using a stored root certificate.

Updating the BlackBerry Device Software from an update web site

You can configure the IT policy rules that are included in the Wired Software Updates policy group to permit a user to update the BlackBerry Device Software from an update web site using the BlackBerry Desktop Manager or BlackBerry Application Web Loader. The user can use the update process to update the BlackBerry Device Software from a computer that is outside your organization's network (for example, from home).

During the update process, a BlackBerry device activates itself automatically over the wireless network so that the user can use a computer that is outside your organization's network to update the BlackBerry Device Software. When a user who does not use the BlackBerry Desktop Manager visits the update web site, the user must download and install Microsoft ActiveX components on the computer before the user can update the BlackBerry Device Software. The update process can take from 15 minutes to 2 hours, depending on the type of update, amount of device data, and number of applications that are installed on the device. A user cannot use the device or make emergency calls during the update process.

BlackBerry Device Software versions 5.0 and later, BlackBerry Desktop Manager versions 5.0.1 and later, and BlackBerry Application Web Loader versions 1.1.0 and later support BlackBerry Device Software updates from an update web site.

For more information about the IT policy rules that are included in the Wired Software Updates policy group, see the *BlackBerry Enterprise Server Policy Reference Guide*. For more information about the BlackBerry Application Web Loader, see the *BlackBerry Application Web Loader Developer Guide*.

Protecting cryptographic services data when updating the BlackBerry Device Software from an update web site

When a user updates the BlackBerry Device Software from an update web site, the BlackBerry Enterprise Solution backs up cryptographic services data (for example, cryptographic keys and service books) from a BlackBerry device to the user's

computer. To protect the cryptographic services data, the device encrypts the cryptographic services data using a BlackBerry services key.

The device stores the BlackBerry services key in the NV store in flash memory. Neither the user nor third-party applications can access the location in the NV store where the device stores the BlackBerry services key. If you or a user turns on content protection, the device also encrypts the BlackBerry services key using the content protection key.

After the device encrypts the cryptographic services data, the BlackBerry Desktop Manager or BlackBerry Application Web Loader backs up the encrypted cryptographic services data to a database and stores the database on the user's computer as an .ipd file.

When the update process completes, the BlackBerry Desktop Manager or BlackBerry Application Web Loader restores the cryptographic services data to the device. Only the device that encrypted the cryptographic services data can decrypt the cryptographic services data. The device can decrypt the cryptographic services data only once. The device deletes the BlackBerry services key from the NV store after the device decrypts the cryptographic services data.

The BlackBerry Enterprise Solution does not back up or restore cryptographic services data except during the BlackBerry Device Software update process from an update web site. When the user backs up or restores device data by selecting the backup and restore options in the BlackBerry Desktop Manager, the back up and restore processes do not access cryptographic services data.

Data flow: Generating a BlackBerry services key that protects cryptographic services data

The BlackBerry device uses an ephemeral AES-256 encryption key (called the BlackBerry services key) to encrypt the cryptographic services data. To generate the BlackBerry services key, the device performs the following actions:

1. generates a random password from a random source of 32 bytes
2. generates a random salt from a random source of 8 bytes
3. concatenates the salt, password, and salt again into a byte array (for example, `Salt|Password|Salt`)
4. hashes the byte array using SHA-256
5. stores the resulting hash in a byte array that is called a key

```
(key) =
SHA256(Salt|Password|Salt)
```

6. hashes the key 18 more times and stores the result in a key each time

   For example, for i=0 to 18, the device performs the following actions:

```
(key) = SHA256(key)
 i++
 done
```

   The final hash creates the BlackBerry services key.

7. stores the BlackBerry services key in a location of the NV store that third-party applications and the user cannot access

Data flow: Backing up cryptographic services data using the BlackBerry Desktop Manager

1. A user connects a BlackBerry device to the BlackBerry Desktop Manager and selects the option to update the BlackBerry Device Software.
2. The BlackBerry Desktop Manager determines that cryptographic services data require backup during the update process. It sends the device a command to encrypt the cryptographic services data.
3. The device performs the following actions:
   a. generates a BlackBerry services key and stores the BlackBerry services key in the NV store
   b. encrypts the cryptographic services data using the BlackBerry services key
   c. encrypts the BlackBerry services key using the content protection key if you or the user turns on content protection
4. The BlackBerry Desktop Manager backs up the encrypted cryptographic services data in a database on the user's computer as an .ipd file.

Data flow: Restoring cryptographic services data using the BlackBerry Desktop Manager or BlackBerry Application Web Loader

1. After the update process completes, the BlackBerry Desktop Manager or BlackBerry Application Web Loader determines that cryptographic services data must be restored to the BlackBerry device. The BlackBerry Desktop Manager or BlackBerry Application Web Loader sends a device a command to restore the cryptographic services data.
2. The device performs the following actions:
   a. retrieves the BlackBerry services key and verifies that the BlackBerry services key was not used previously
   b. decrypts the BlackBerry services key if you or a user turn on content protection
3. The BlackBerry Desktop Manager restores the encrypted cryptographic services data to the device.
4. The device performs the following actions:
   a. decrypts the encrypted cryptographic services data using the BlackBerry services key
   b. restores the decrypted cryptographic data
   c. deletes the BlackBerry services key from the NV store

Extending messaging security to a device

15

If your organization's messaging environment supports highly secure messaging technology such as PGP encryption or S/MIME encryption, you can configure the BlackBerry Enterprise Solution to encrypt a message using PGP encryption or S/MIME encryption so that the message remains encrypted when the BlackBerry Enterprise Server forwards the message to the email applications of recipients. To extend messaging security, the sender and recipient must install highly secure messaging technology on the computers that host the email applications and on their BlackBerry devices, and you must configure the devices to use the highly secure messaging technology.

Extending messaging security using PGP encryption

You can extend messaging security for the BlackBerry Enterprise Solution and permit a BlackBerry device user to send and receive PGP protected email messages and PGP protected PIN messages on a BlackBerry device. The BlackBerry Enterprise Solution supports the OpenPGP format and PGP/MIME format on the device.

To extend messaging security, you must instruct the device user to install the PGP Support Package for BlackBerry smartphones on the device and to transfer the PGP private key of the device user to the device. The device user can use the PGP private key to digitally sign, encrypt, and send PGP protected messages from the device. If a device user does not install the PGP Support Package for BlackBerry smartphones, the device displays an error message when the device user tries to open PGP protected messages.

To require the device user to use PGP encryption when forwarding or replying to messages, you can configure the PGP Force Digital Signature IT policy rule and the PGP Force Encrypted Messages IT policy rule.

The PGP Support Package for BlackBerry smartphones is designed to support encoding and decoding Unicode messages and permits PGP encryption using keys or passwords. The PGP Support Package for BlackBerry smartphones permits the device to encrypt PGP protected email messages or PGP protected PIN messages using a password that the sender and recipient both know.

For more information about the OpenPGP format, see RFC 2440. For more information about the PGP/MIME format, see RFC 3156.

PGP public keys and PGP private keys

The PGP Support Package for BlackBerry smartphones uses public key cryptography with PGP public keys and PGP private keys.

Key	Description
PGP public key	The PGP Support Package for BlackBerry smartphones uses the PGP public key of the recipient to encrypt outgoing email messages and the PGP public key of the sender to verify digital signatures on incoming email messages. The PGP public key is designed so that recipients and senders can distribute and access the key without compromising it. The PGP public key is stored typically on the PGP Universal Server or an LDAP server.
PGP private key	The PGP Support Package for BlackBerry smartphones uses the PGP private key of the sender to digitally sign outgoing email messages and the PGP private key of the recipient to decrypt incoming email messages. To make sure that security is not compromised, you must make sure that private key information remains private to the key owner. The BlackBerry device stores the PGP private key.

Retrieving PGP keys from a PGP Universal Server or LDAP servers

If your organization's environment includes a PGP Universal Server, the administrator of the PGP Universal Server can configure the email policy of the PGP Universal Server. After a user installs the PGP Support Package for BlackBerry smartphones, a BlackBerry device can retrieve and enforce the email policy of the PGP Universal Server for all email messages that the user sends.

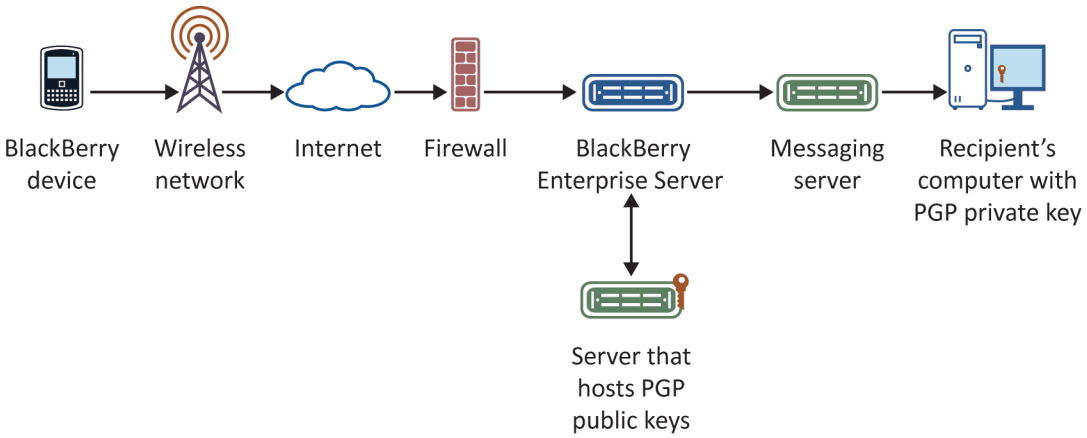
The device is designed to use the BlackBerry MDS Connection Service to connect to the PGP Universal Server or any LDAP server that a user specifies on the device or that you specify using the BlackBerry Administration Service. The BlackBerry MDS Connection Service uses standard protocols, such as HTTP and TCP/IP, to permit the device to retrieve PGP public keys, PGP key status, and X.509 certificate status from the PGP Universal Server or an LDAP server over the wireless network. The BlackBerry MDS Connection Service can connect to LDAP servers using LDAPS.

Encryption algorithms that the device supports for PGP encryption

When you turn on PGP encryption, the default value of the PGP Allowed Content Ciphers IT policy rule specifies that a BlackBerry device can use any of the following encryption algorithms to encrypt email messages and PIN messages: AES-256, AES-192, AES-128, CAST-128, or Triple DES-168. You can change the value to use a subset of the encryption algorithms if your organization's security policies require it.

The PGP public key of the recipient indicates which encryption algorithm the recipient's email application supports, and the device is designed to use that encryption algorithm. By default, if the PGP public key of the recipient does not include a list of encryption algorithms, the device encrypts the email message or PIN message using Triple DES.

Data flow: Sending an email message using PGP encryption



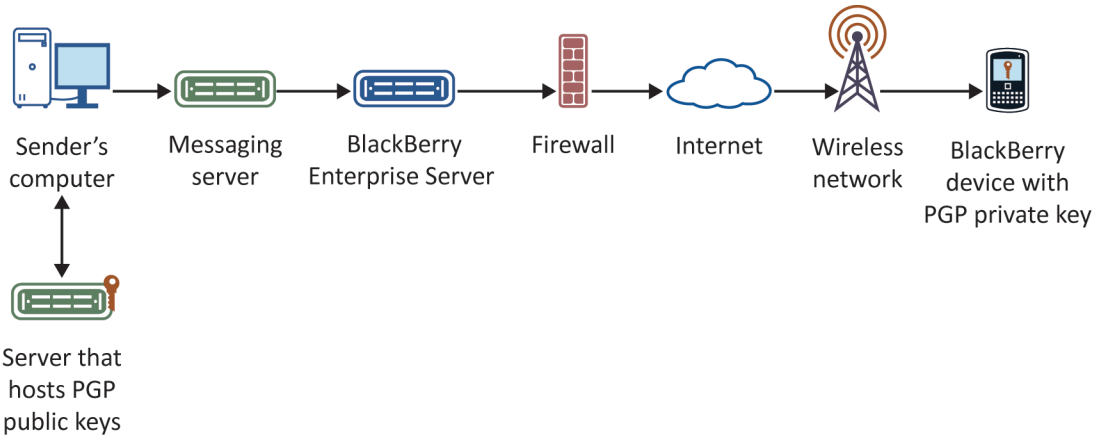
If a sender installs the PGP Support Package for BlackBerry smartphones on a BlackBerry device, the device encrypts outgoing email messages.

1. The device performs the following actions:
   a. uses the BlackBerry MDS Connection Service to retrieve the PGP public key of the recipient from the PGP Universal Server or LDAP server
   b. encrypts the email message using the PGP public key of the recipient
   c. uses BlackBerry transport layer encryption to encrypt the PGP encrypted message

d sends the message that is encrypted using BlackBerry transport layer encryption and PGP encryption to the BlackBerry Enterprise Server

2. The BlackBerry Enterprise Server removes the BlackBerry transport layer encryption and sends the PGP encrypted message to the recipient.

Data flow: Receiving a PGP encrypted message



If a recipient installs the PGP Support Package for BlackBerry smartphones on a BlackBerry device, the device decrypts incoming PGP encrypted messages.

1. A sender uses the PGP technology on the email application to encrypt an email message using the PGP public key of the recipient.
2. The BlackBerry Enterprise Server performs the following actions:
   a retrieves the email message from the messaging server
   b uses BlackBerry transport layer encryption to encrypt the PGP encrypted message
   c sends the email message encrypted using BlackBerry transport layer encryption and PGP encryption to the device
3. The device performs the following actions:
   a decrypts the BlackBerry transport layer encryption and stores the PGP encrypted message in the flash memory of the device
   b decrypts the PGP encrypted message using the PGP private key of the recipient and displays the contents of the email message when the recipient opens the email message on the device

Extending messaging security using S/MIME encryption

You can extend messaging security for the BlackBerry Enterprise Solution and permit a BlackBerry device user to send and receive S/MIME-protected email messages and S/MIME-protected PIN messages on a BlackBerry device.

To extend messaging security, you or the device user must install the S/MIME Support Package for BlackBerry smartphones on the device and transfer the S/MIME private key of the device user to the device. The S/MIME Support Package for BlackBerry smartphones is designed to work with email applications such as Microsoft Outlook, Microsoft Outlook Express, and IBM Notes, and with PKIs such as Netscape, Entrust Authority Security Manager version 5 and later, and Microsoft certification authorities.

The device user uses the S/MIME private key to decrypt S/MIME-protected messages on the device and to sign, encrypt, and send S/MIME-protected messages from the device. If the BlackBerry Enterprise Server receives an S/MIME-encrypted message but the device user did not install the S/MIME Support Package for BlackBerry smartphones, the BlackBerry Enterprise Server sends a message to the device to indicate that the device does not support S/MIME-encrypted messages.

After the device user installs the S/MIME Support Package for BlackBerry smartphones, the device user can synchronize and manage S/MIME certificates and S/MIME private keys using the certificate synchronization tool of the BlackBerry Desktop Manager. The BlackBerry Enterprise Server does not apply an appended disclaimer to S/MIME-protected messages that the device user sends from the device. Digital signatures on S/MIME-protected messages that the device sends are not valid if disclaimers are appended to the messages.

To require the device user to use S/MIME encryption when forwarding or replying to messages, you can configure the S/MIME Force Digital Signature IT policy rule and the S/MIME Force Encrypted Messages IT policy rule.

The S/MIME Support Package for BlackBerry smartphones is also designed to support the following features:

- encoding and decoding of Unicode messages
- ability to use a password, which the sender and recipient each know, to encrypt S/MIME-protected email messages or PIN messages
- ability to read S/MIME certificates that are stored on a smart card

S/MIME certificates and S/MIME private keys

The S/MIME Support Package for BlackBerry smartphones uses public key cryptography with S/MIME certificates and S/MIME private keys to encrypt and decrypt email messages and PIN messages. The S/MIME Support Package for BlackBerry smartphones use PKI protocols to search for and retrieve S/MIME certificates and certificate status over the wireless network.

Item	Description
S/MIME certificate	When a user sends an email message or PIN message from a BlackBerry device, the device uses the S/MIME certificate of the recipient to encrypt the message. When a user receives a signed email message or signed PIN message on a device, the device uses the S/MIME certificate of the sender to verify the message signature.
S/MIME private key	When a user sends a signed email message or signed PIN message from a device, the device hashes the message using SHA-1, SHA-2, or MD5. The device then uses the S/MIME private key of the user to digitally sign the message hash. When a user receives an encrypted email message or encrypted PIN message on a device, the device uses the private key of the user to decrypt the message. The device stores the private key.

Retrieving S/MIME certificates and checking certificate status

The S/MIME Support Package for BlackBerry smartphones is designed so that the BlackBerry device and the certificate synchronization tool of the BlackBerry Desktop Manager can perform the following actions:

- use LDAP, LDAPS, or DSML to search for and retrieve S/MIME certificates of recipients from LDAP servers or DSML certificate servers
- use OCSP to check the revocation status of S/MIME certificates
- retrieve the revocation status of S/MIME certificates from a certificate revocation list

S/MIME encryption algorithms

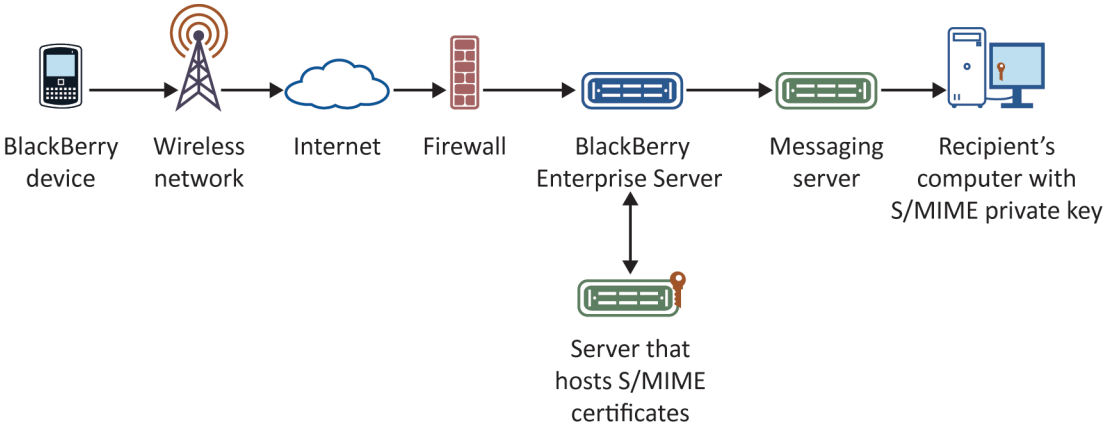
When you turn on S/MIME encryption, the default value of the S/MIME Allowed Content Ciphers IT policy rule specifies that a BlackBerry device can use any of the following encryption algorithms to encrypt messages: AES-256, AES-192, AES-128, CAST-128, RC2-128, or Triple DES. By default, the device cannot use the RC2-64 algorithm and RC2-40 algorithm to encrypt S/MIME messages. You can change the value of the S/MIME Allowed Content Ciphers IT policy rule to use a subset of the encryption algorithms if your organization's security policies require it.

If a BlackBerry device user wants to send an email message to a recipient that the user previously received an email message from, the device is designed to store the encryption algorithms that the recipient's email application can support, and use one of those encryption algorithms. By default, if the device cannot determine the encryption algorithms that the recipient's email application can support, the device encrypts the email message using Triple DES.

You can use the Weak Digest Algorithms IT policy rule to specify the algorithms that your organization considers to be weak. The device uses the list of weak algorithms in the Weak Digest Algorithms IT policy rule when the device verifies the following information:

- An S/MIME-enabled application did not use a weak algorithm to generate the digital signatures on the email messages that the device receives.
- The certificate chains for the certificates that an S/MIME-enabled application used to digitally sign email messages that the device receives do not contain hash values generated using a weak algorithm.

Data flow: Sending an email message using S/MIME encryption

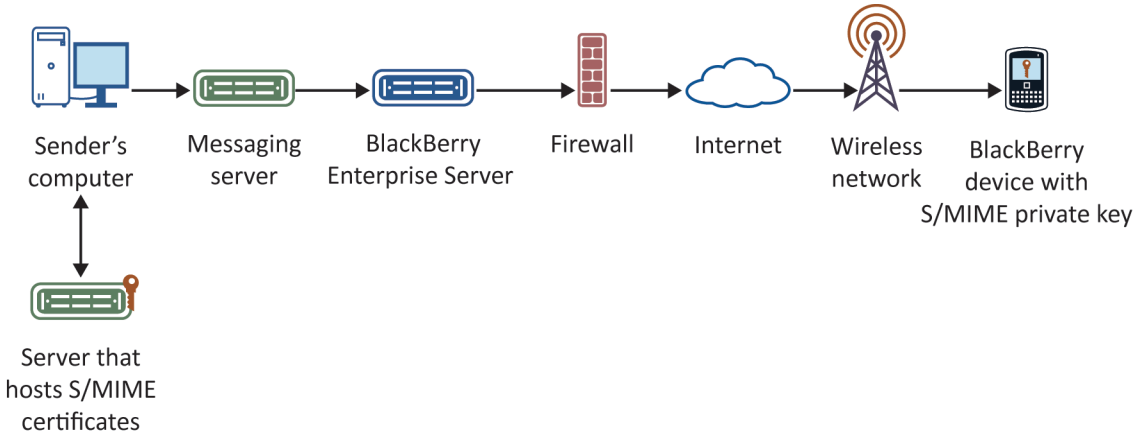


If a sender installs the S/MIME Support Package for BlackBerry smartphones on a BlackBerry device, the device encrypts outgoing email messages.

1. The device performs the following actions:
   a. checks the BlackBerry device key store for the S/MIME certificate of the recipient
   b. if the BlackBerry device key store does not include the S/MIME certificate of the recipient, uses the BlackBerry MDS Connection Service to retrieve the S/MIME certificate of the recipient from the LDAP server or DSML server and verify the certificate status
   c. encrypts the email message with the S/MIME certificate of the recipient or a password that the sender specifies
   d. if the sender specifies a password, combines the password with random bytes to generate an encryption key that is specific to S/MIME encryption
   e. uses BlackBerry transport layer encryption to encrypt the S/MIME-encrypted message
   f. sends the message that is encrypted using BlackBerry transport layer encryption and S/MIME encryption to the BlackBerry Enterprise Server
2. The BlackBerry Enterprise Server decrypts the BlackBerry transport layer encryption and sends the S/MIME-encrypted message to the recipient.

3. The recipient decrypts the S/MIME-encrypted message using the S/MIME private key or a password that the sender provides.

Data flow: Receiving an S/MIME-encrypted email message



If a recipient installs the S/MIME Support Package for BlackBerry smartphones, the BlackBerry device decrypts incoming email messages.

1. The sender uses the S/MIME technology on the email application to encrypt the email message using the S/MIME certificate of the recipient.
2. The BlackBerry Enterprise Server performs the following actions:
   a retrieves the S/MIME-encrypted message from the messaging server
   b encrypts the email message a second time with S/MIME encryption if the email message is signed-only or weakly encrypted and if you turned on the Turn on S/MIME encryption on signed and weakly encrypted messages option in the BlackBerry Administration Service
   c uses BlackBerry transport layer encryption to encrypt the S/MIME-encrypted message
   d sends the email message that is encrypted using BlackBerry transport layer encryption and S/MIME encryption to the device
3. The device decrypts the BlackBerry transport layer encryption and stores the S/MIME-encrypted message in BlackBerry device memory.
4. When the recipient opens the email message on the device, the device decrypts the S/MIME-encrypted message using the S/MIME private key of the recipient and displays the message contents. If the email message is encrypted with a password, the recipient types the password to decrypt the S/MIME-encrypted message.

Extending messaging security using IBM Notes encryption

By default, if your organization's environment includes IBM Notes API version 7.0 or later and either BlackBerry Enterprise Server version 4.1 or later for IBM Domino or the BlackBerry Enterprise Server Express for IBM Domino 5.0 SP2 or later, a BlackBerry device can decrypt messages that are encrypted using Notes encryption.

If your organization's environment includes BlackBerry Enterprise Server version 5.0 or later or BlackBerry Enterprise Server Express version 5.0 SP2 or later, a user with BlackBerry Device Software version 5.0 or later, can encrypt messages using Notes encryption. When the user creates, forwards, or replies to a message, the user can indicate whether the BlackBerry Enterprise Server or BlackBerry Enterprise Server Express must encrypt the message before it sends the message to the recipients.

To use Notes encryption on the device, the device user must import a copy of the Notes .id file into the user's message database using the BlackBerry Desktop Software or iNotes. If your organization's environment includes Domino version 8.5.1 or later and either BlackBerry Enterprise Server version 5.0 SP1 or later or BlackBerry Enterprise Server Express 5.0 SP2 or later, you can configure the BlackBerry Enterprise Server or BlackBerry Enterprise Server Express to import the Notes .id file automatically into the user's message database from the Notes ID vault.

To require the user to use Notes encryption when forwarding or replying to messages, you can configure the Require Notes Native Encryption For Outgoing Messages IT policy rule. To prevent a user from forwarding or replying to Notes protected messages, you can configure the Disable Notes Native Encryption Forward And Reply IT policy rule.

Protecting the password for an IBM Notes .id file

How a device protects the password for an IBM Notes .id file

After a user imports an IBM Notes .id file and password for the Notes .id file to the user's message database, the device encrypts the password in device memory using AES encryption and the device transport key. The device decrypts the password before it calls the required security functions in the Notes API.

The device deletes the plain-text password from the device memory when it receives a notification from the BlackBerry Enterprise Server that the BlackBerry Enterprise Server cannot decrypt a message, when the device resets, or when the Notes password expires. (The default expiration period is 24 hours.) You can use the Native Encryption Password Timeout IT policy rule to specify the maximum duration (in minutes) that the device stores the plain-text password for the Notes .id file.

You can change the timeout value to 0 to require the user to type the password to decrypt each Notes encrypted email message that the user receives on the device.

When Notes encryption is not available, the user can turn on Notes encryption manually by importing the Notes .id file or by changing the password using the BlackBerry Desktop Software or IBM Domino Web Access client.

How the BlackBerry Messaging Agent protects the password for an IBM Notes .id file

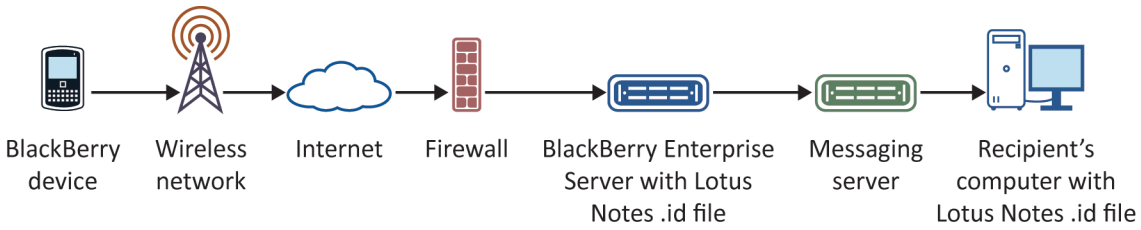
After a user imports an IBM Notes .id file and the password for the Notes .id file to the user's message database, the BlackBerry Messaging Agent encrypts the Notes .id file and password in the BlackBerry Messaging Agent memory cache using AES encryption and the device transport key.

The BlackBerry Messaging Agent deletes the Notes .id file and the plain-text password when the BlackBerry Enterprise Server cannot decrypt a message, when the BlackBerry Enterprise Server restarts, or when the password expires. (The default timeout value is 24 hours.)

The BlackBerry Messaging Agent does not delete the encrypted password in the BlackBerry Messaging Agent memory cache. You can change the duration that the BlackBerry Messaging Agent caches the password for. For information about changing the duration that the BlackBerry Messaging Agent caches the password for, visit www.blackberry.com/support to read article KB12420.

If the user types a password incorrectly more than 10 times consecutively within 1 hour, the BlackBerry Messaging Agent makes secure messaging unavailable for 1 hour. This period increases each time that the user exceeds the maximum number of unsuccessful password attempts. The period increases by 10-minute increments to a maximum of 24 hours. When the user types the password correctly, the BlackBerry Messaging Agent restores the default value of 1 hour.

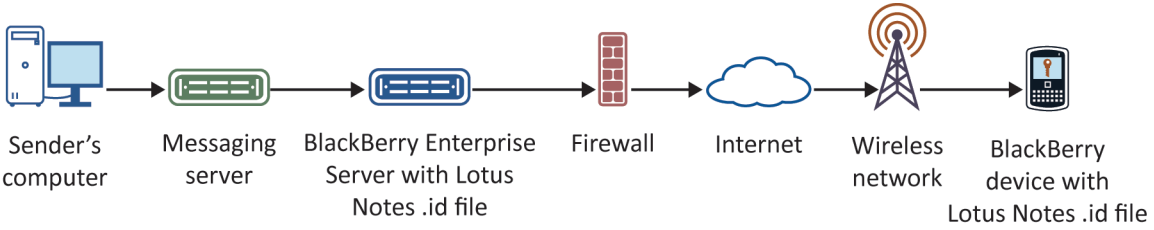
Data flow: Sending an email message using IBM Notes encryption



1. A user indicates, using the menu in the messages application, that the BlackBerry device must encrypt the email message.
2. The device performs the following actions:
   a prompts the user for the password for the IBM Notes .id file
   b configures the email message for Notes encryption
   c encrypts the email message using BlackBerry transport layer encryption
   d sends the email message and password to the BlackBerry Enterprise Server
3. The BlackBerry Enterprise Server decrypts the email message using BlackBerry transport layer encryption.

4. The BlackBerry Messaging Agent on the BlackBerry Enterprise Server decrypts the cached password for the Notes .id file and validates the password that the device sent. If the BlackBerry Messaging Agent can verify the password, the BlackBerry Messaging Agent uses the password to encrypt the message using Notes encryption.
5. The BlackBerry Enterprise Server sends the encrypted email message to the messaging server so that the messaging server can deliver it to the recipient.

Data flow: Receiving an IBM Notes encrypted message



1. A user uses the IBM Notes application on the user's computer to encrypt a message using the password for the Notes .id file.
2. The BlackBerry Enterprise Server performs the following actions:
   a retrieves the Notes encrypted message from the messaging server
   b encrypts the Notes encrypted message using BlackBerry transport layer encryption
   c sends the encrypted message to the BlackBerry device
3. The device decrypts the message using BlackBerry transport layer encryption and stores the message without decrypting the Notes encryption.
4. The user tries to open the Notes encrypted message on the device.
5. The BlackBerry Messaging Agent on the BlackBerry Enterprise Server decrypts the cached password for the Notes .id file and uses the password to decrypt the message. If the BlackBerry Messaging Agent does not have the password, from the menu in the messages application, the user must select More, More All, or Open Attachment to send the decrypted message to the device.
6. The BlackBerry Enterprise Server deletes the decrypted password from the BlackBerry Messaging Agent memory cache and sends the decrypted message to the device.

Extending messaging security for attachments

The BlackBerry Enterprise Server supports attachments in PGP protected messages and S/MIME-protected messages. It also permits a BlackBerry device user to view encrypted attachments on a BlackBerry device. For PGP protected messages, the device supports OpenPGP format and PGP/MIME format. For S/MIME-protected messages, the device supports Triple DES, AES-128, AES-192 or AES-256.

You can use the PGP Allowed Encrypted Attachment Mode IT policy rule and the S/MIME Allowed Encrypted Attachment Mode IT policy rule to control whether users can view encrypted attachments on their devices. By default these rules permit a device to request decrypted attachment information from the BlackBerry Enterprise Server automatically when a user opens a protected message.

On a device that is running BlackBerry 7 or later in a Microsoft Exchange environment, you can use the S/MIME Attachment Support IT policy rule to control whether users can send and forward attachments in S/MIME-protected messages. The S/MIME Attachment Support IT policy rule can be set to one of the following values:

- **None**, which prevents the device from sending attachments in S/MIME-protected messages.
- **End-to-End**, which permits the device to send attachments in new S/MIME-protected messages that the sender composes, if the attachments are located on the sender's device.
- **End-to-End or Trusted BES**, which permits the device to send attachments in S/MIME-protected messages whether or not the attachments are located on the sender's device.

By default, the "End-to-End or Trusted BES" value is configured for this rule.

Data flow: Viewing an attachment in a PGP encrypted message or S/MIME-encrypted message

The S/MIME Allowed Encrypted Attachment Mode IT policy rule or PGP Allowed Encrypted Attachment Mode IT policy rule determines how a BlackBerry device responds when it receives a PGP/MIME encrypted message or S/MIME-encrypted message that contains an attachment. These rules determine whether the following actions occur automatically when the user opens the email message, or whether the user must request the actions manually.

1. A device sends the message key and a request for the data in the attachment header to the BlackBerry Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the email message and access the data in the attachment header. The BlackBerry Enterprise Server sends the data in the attachment header to the device.
3. The device processes the data in the attachment header with the email message and displays the associated attachment information so that the user can select the attachment for viewing.

Data flow: Viewing an attachment that is encrypted using S/MIME encryption, PGP/MIME encryption, or OpenPGP encryption

1. The BlackBerry device sends the message key and a request for the attachment data to the BlackBerry Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the email message and access the attachment data that corresponds to the data in the attachment header. The BlackBerry Enterprise Server decrypts the attachment and sends the rendered attachment data to the device.
3. The device displays the attachment.

To help protect the decrypted attachment data that the device stores, you can turn on content protection.

Data flow: Sending an S/MIME-protected email message that contains attachments that are located on a device

On a BlackBerry device that is running BlackBerry 7 or later in a Microsoft Exchange environment, you can use the S/MIME Attachment Support IT policy rule.

The S/MIME Attachment Support IT policy rule determines how a device responds when a BlackBerry device user sends a new S/MIME-protected message with an attachment, forwards an S/MIME-protected message with an attachment, or replies to an S/MIME-protected email message with an attachment. By default, this rule is set to the "End-to-End or Trusted BES" value. When the user composes and sends an S/MIME-protected message that includes attachments that are located on the device, it uses End-to-End mode. In all other scenarios (even when a user forwards an S/MIME-protected message after downloading the original message attachment to the device), the device uses Trusted BES mode.

1. A user performs the following actions when the user composes an email message:
   a. Attaches at least one file to the email message
   b. Selects the S/MIME encoding action for the email message (for example, sign, encrypt, or sign and encrypt using S/MIME)
   c. Sends the email message
2. The email application on the device performs the following actions:
   a. Generates an email message including attachments
   b. Encrypts, signs, or encrypts and signs the email message using S/MIME

c Sends the email message to the BlackBerry Enterprise Server

3. The BlackBerry Enterprise Server sends the email to the recipient's inbox.

Data flow: Forwarding an S/MIME-protected email message that contains attachments that are not located on a device

On a BlackBerry device that is running BlackBerry 7 or later in a Microsoft Exchange environment, you can use the S/MIME Attachment Support IT policy rule.

The S/MIME Attachment Support IT policy rule determines how a device responds when a BlackBerry device user sends a new S/MIME-protected email message with an attachment, forwards an S/MIME-protected email message with an attachment, or replies to an S/MIME-protected email message with an attachment. By default, this rule is set to the "End-to-End or Trusted BES" value, which means the device can forward email messages with attachments whether or not the attachments are located on the device. When the device forwards encrypted email messages that include attachments that are not located on the device, it uses Trusted BES mode.

1. A user performs the following actions when the user forwards a message:
   a Selects whether the message should be signed, encrypted, or signed and encrypted using S/MIME
   b If applicable, attaches any new message attachments
   c Sends the message
2. The email application on the device performs the following actions:
   a Creates a message header that contains information about whether the user wants the forwarded message to be signed, encrypted, or signed and encrypted using S/MIME. If the original message that the user forwards was encrypted, the message header includes a key for decrypting the original message.
   b Sends the partial message, which includes the new message body, any new attachments that are located on the device, and the message header, to the BlackBerry Enterprise Server.
3. The BlackBerry Enterprise Server performs the following actions when it receives the partial message:
   a Parses the message header
   b Obtains the original message and performs one of the following actions:
      - If the original sender signed the message that a user is forwarding, removes all of the original signatures
      - If the original sender encrypted the message that a user is forwarding, decrypts the message using the key in the message header
      - If the original sender signed and encrypted the message that a user is forwarding, decrypts the message using the key in the message header and then removes all of the original signatures

c Appends all of the attachments from the original message, any new message attachments, and the original message body to the new message

d If the user indicates that the new message must be signed, sends a Message Signature Request to the device, waits for a reply from the device, and adds the signature into the message

e If the user indicates that the new message must be encrypted, encrypts the full message

f Sends the message to the recipient's inbox

16 Configuring two-factor authentication and protecting Bluetooth connections

BlackBerry Smart Card Reader

The BlackBerry Smart Card Reader is an accessory that, when used in proximity to a Bluetooth enabled BlackBerry device or a Bluetooth enabled computer, permits a user to authenticate with a smart card and log in to the BlackBerry device or computer.

The BlackBerry Smart Card Reader is designed to perform the following actions:

- communicate with BlackBerry devices and computers using Bluetooth technology version 1.1 or later and, by default, use AES-256 encryption on the application layer
- permit a user to use two-factor authentication to access BlackBerry services and PKI applications
- permit a user to digitally sign and encrypt email messages and receive encrypted messages on the BlackBerry device when the user installs the S/MIME Support Package for BlackBerry smartphones
- store all encryption keys in RAM only and never write the keys to flash memory

The BlackBerry Smart Card Reader permits a user to prove the user's identity to the BlackBerry device or a computer using what the user has (smart card) and what the user knows (smart card password).

For more information, see the *BlackBerry Smart Card Reader Security Technical Overview*.

Advanced Security SD cards

Similar to the BlackBerry Smart Card Reader, an Advanced Security SD card permits a user to prove the user's identity to the BlackBerry device using what the user has (smart card) and what the user knows (smart card password). The BlackBerry Enterprise Solution supports Advanced Security SD cards that use the security system for the MCEX smart card.

You can configure a BlackBerry device to require that a user uses an Advanced Security SD card to perform the following actions:

- unlock the BlackBerry device and access BlackBerry services and PKI applications using two-factor authentication
- digitally sign and encrypt email messages and PIN messages using S/MIME encryption when the user installs the S/MIME Support Package for BlackBerry smartphones on the BlackBerry device
- decrypt S/MIME-encrypted email messages and PIN messages
- import certificates that are stored on the Advanced Security SD card into the NV store of the BlackBerry device flash memory
- open SSL connections

To configure the BlackBerry device to support an Advanced Security SD card, a user must insert the Advanced Security SD card into the BlackBerry device and install the smart card driver of the Advanced Security SD card on the BlackBerry device using the BlackBerry Desktop Manager. After the user installs the smart card driver on the BlackBerry device, the user can configure the driver settings in the security options, on the Smart Card screen.

To control how a BlackBerry device can use an Advanced Security SD card, you can use the Force Smart Card Two-Factor Authentication IT policy rule, Force Smart Card Two Factor Challenge Response IT policy rule, or Disable Certificate or Key Import From External Memory IT policy rule.

To permit third-party applications on the BlackBerry device to access the Advanced Security SD card, a developer can use the SmartCard API in the BlackBerry Java Development Environment.

BlackBerry Device Software versions 5.0 and later support Advanced Security SD cards.

For more information about configuring the BlackBerry device to support an Advanced Security SD card, see the user guide for the BlackBerry device. For more information about using IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Two-factor authentication

You can use the BlackBerry Smart Card Reader or an Advanced Security SD card to require a user to use a smart card and the smart card password to prove the user's identity before the BlackBerry device unlocks. If a user installs a smart card authenticator, smart card driver, and the driver for the smart card reader on the BlackBerry device, you or the user can configure two-factor authentication on the BlackBerry device to bind the BlackBerry device to the installed smart card. After the BlackBerry device binds to the smart card, the BlackBerry device requires the user to use the smart card to authenticate before the BlackBerry device unlocks.

To require that a user authenticate with the BlackBerry device using the smart card, you can configure the Force Smart Card Two-Factor Authentication IT policy rule in the BlackBerry Administration Service. If you do not require the user to authenticate with the BlackBerry device using a smart card, the user can turn on or turn off two-factor authentication in the BlackBerry device options, in the security options, in the User Authenticator field.

Verifying that a device is bound to a smart card

After a user turns on two-factor authentication, the BlackBerry device prompts the user to insert the smart card into the BlackBerry Smart Card Reader. The device displays the label and card type of the bound smart card.

If the device is running BlackBerry Device Software version 3.6, the smart card information that the device displays when it prompts the user to insert the smart card into the BlackBerry Smart Card Reader is the only indication that a smart card is bound to the device.

If the device is running BlackBerry Device Software version 4.0 or later, the device displays the smart card information when it prompts the user to insert the smart card. The user can view the smart card information in the device options, in the security options. The Initialized field specifies whether the device authenticated with and is bound to the smart card.

Data flow: Turning on two-factor authentication using a smart card

When you or a user turns on two-factor authentication with the BlackBerry Smart Card Reader, the BlackBerry device performs the following actions:

1. locks
2. prompts the user to type the BlackBerry device password when the user tries to unlock the BlackBerry device
3. requires the user to specify a BlackBerry device password, if the user has not yet specified one
4. prompts the user to type the smart card password to turn on two-factor authentication using the smart card
5. binds to the smart card by storing the following binding information in the NV store in the BlackBerry device memory that the user cannot access:
    - name of a class that the BlackBerry Smart Card Reader requires
    - binding information format for the smart card type (for example, the type for CAC is GSA CAC)
    - name of a Java class that the smart card code requires
    - unique 64-bit identifier that the smart card provides
    - smart card label that the smart card provides (for example, HISLOP.GREG.1234567890)
6. pushes the current IT policy to the BlackBerry Smart Card Reader

Creating two-factor authentication methods

The BlackBerry Java Development Environment version 5.0 includes the User Authenticator API that a developer can use to create two-factor authentication methods. A user can use the two-factor authentication methods with the BlackBerry device password to unlock a BlackBerry device. After the developer creates an authentication method using the User Authenticator API, you can install the authentication method on the BlackBerry device using a software configuration.

To configure the BlackBerry device so that the user must provide the BlackBerry device password and authenticate using a two-factor authentication method before the BlackBerry device unlocks, you change the Allowed Authentication Mechanisms IT policy rule to Other and configure the Is Access to the User Authenticator API Allowed application control policy rule.

The User Authenticator API permits a developer to add a field to the password dialog box on the BlackBerry device for the authentication method. You can create as many two-factor authentication methods as the security policies of your organization require.

BlackBerry Device Software versions 5.0 and later support the User Authenticator API.

For more information about the User Authenticator API, see the *BlackBerry Java Development Environment Fundamentals Guide*.

Two-factor content protection

Two-factor content protection on the BlackBerry device is designed to protect the content protection decryption keys with both a private key that is stored on a smart card and the device password.

To store the private key, you can use either a smart card with the BlackBerry Smart Card Reader or an Advanced Security SD card. The content protection key is not transferred from the device to the BlackBerry Smart Card Reader or Advanced Security SD card.

Two-factor content protection requires the device password, a smart card, and an authentication certificate that is stored on the device. The authentication certificate must contain the public key for the private key that is stored on the smart card. If the authentication certificate expires or is revoked, a user can continue to use it for two-factor content protection until the user creates and configures a new certificate to use with two-factor content protection.

You or a user can configure two-factor content protection. By default, if a user has a smart card and an authentication certificate on the device, the user can turn on two-factor content protection. To make two-factor content protection required or optional, or to prevent a user from configuring it, you can use the Two Factor Content Protection Usage IT policy rule. To unlock the device after you or a user turns on two-factor content protection, the user must type the device password and smart card PIN on the login screen in the appropriate fields.

If you or a user turns on two-factor content protection, you cannot change the device password using the BlackBerry Administration Service. Only the user can change the device password on the device.

BlackBerry Device Software 5.0 and later and BlackBerry Smart Card Reader 2.0 and later support two-factor content protection. You must verify that the IT policies that you can use to manage two-factor content protection are available on your organization's BlackBerry Enterprise Server. BlackBerry Enterprise Server 5.0 SP1 and later include the IT policies that you require to manage two-factor content protection.

Data flow: Turning on two-factor content protection

1. When you or a BlackBerry device user turns on two-factor content protection on the BlackBerry device for the first time, the device performs the following actions:
   a. generates a random 256-bit symmetric key for the smart card authenticator
   b. derives an ephemeral AES-256 key from the symmetric key for the smart card authenticator and the device password, using PKCS #5
   c. uses the ephemeral key to encrypt the content protection key and ECC private keys

   d stores the encrypted content protection key and encrypted ECC private keys in the device memory
   e generates a 256-bit pseudorandom number
   f computes the SHA-256 hash of the pseudorandom number and uses it to encrypt the symmetric key for the smart card authenticator, and stores the symmetric key for the smart card authenticator in the device memory
   g encrypts the pseudorandom number using the public key in the authentication certificate that you configured for use with two-factor content protection, and stores the encrypted pseudorandom number in the device memory
   h discards the pseudorandom number, the SHA-256 hash of the pseudorandom number, the ephemeral key, and the key for the smart card authenticator

2. When the device locks, the device discards the content protection key and ECC private keys.
3. When a user unlocks the device, the device retrieves the encrypted copy of the pseudorandom number from the device memory and sends it to the smart card authenticator.
4. The smart card authenticator decrypts the encrypted copy of the pseudorandom number that was stored in the device memory.
5. The device performs the following actions:
   a retrieves the encrypted copy of the key for the smart card authenticator from the device memory and decrypts it using the SHA-256 hash of the decrypted pseudorandom number
   b uses the key for the smart card authenticator and the device password to generate a 256-bit ephemeral key
   c uses the 256-bit ephemeral key to decrypt the ECC private keys and content protection key
   d repeats steps 1e to 1h

The device generates a new pseudorandom number each time the user unlocks the device.

Unbinding a smart card from a device

When you or a BlackBerry device user deletes all device data or turns off two-factor authentication, the BlackBerry device turns off two-factor authentication with the installed smart card and permanently deletes the binding information for the smart card from the device.

The device permanently deletes the binding information for the smart card from the NV store in application storage so that a user can authenticate with the device using a new smart card. You can permanently delete the binding information for the smart card from the device by sending the Delete all device data and remove device IT administration command to the device.

Protecting Bluetooth connections on a device

Bluetooth wireless technology permits a Bluetooth enabled BlackBerry device to open a wireless connection with other Bluetooth devices that are within a 10-meter range (for example, a hands-free car kit or wireless headset).

The device creates a Bluetooth profile, which specifies how applications on the device and on other Bluetooth devices connect and communicate. The device uses the Bluetooth profile to open serial connections to Bluetooth enabled devices using virtual serial ports.

You can use IT policies to manage a Bluetooth enabled device. By default, a Bluetooth enabled device that runs BlackBerry Device Software version 4.0 or later includes the following security measures:

- You or a user can turn off the Bluetooth wireless technology for the device.
- The user must request a connection or pairing on the device with another Bluetooth device and type a passkey (also known as a shared secret key) to complete the pairing.
- The user can specify whether to encrypt data sent to and from the device over a Bluetooth connection. The BlackBerry Enterprise Solution uses the passkey to generate encryption keys.
- The device prompts the user each time a Bluetooth device tries to connect to the device.

For more information, see *Security for BlackBerry Devices with Bluetooth Wireless Technology*.

Using CHAP to open a Bluetooth connection between the BlackBerry Desktop Software and a device

A Bluetooth enabled BlackBerry device can use CHAP to open a Bluetooth connection to the BlackBerry Desktop Software. To open a Bluetooth connection, the device or BlackBerry Desktop Software can use CHAP to send a challenge. The device or BlackBerry Desktop Software can subsequently use the SHA-1 algorithm to calculate a response to the challenge or to validate the response of the other party, depending on which party started the process to open the Bluetooth connection.

When the device uses CHAP, the device never sends the device password over an unprotected connection. The device combines the challenge with the device password to authenticate with the BlackBerry Desktop Software.

For more information about CHAP, see RFC 1994.

Wi-Fi enabled devices

17

Wi-Fi enabled BlackBerry devices permit users with qualifying data plans to access BlackBerry services over a mobile network, Wi-Fi network, or both networks simultaneously.

When users can access a mobile network and Wi-Fi network simulaneously, users can perform multiple tasks over both networks. For example, a user with a BlackBerry 8820 smartphone can send messages over a Wi-Fi network and can make a call over the mobile network at the same time.

If users' mobile network providers make UMA technology (GAN technology) available, and users have subscribed to the UMA feature, Wi-Fi enabled devices can access the mobile network providers' voice services and data services over a mobile network or a Wi-Fi network.

Wi-Fi enabled devices can open a Wi-Fi connection from an enterprise Wi-Fi network or, with a VPN session, from a home Wi-Fi network or Wi-Fi hotspot to connect directly to the BlackBerry Router.

Wi-Fi enabled devices are designed to open a connection to the BlackBerry Internet Service to access the BlackBerry MDS Connection Service, BlackBerry Messenger, and other devices for PIN messaging. You can verify with your organization's wireless service provider whether your organization's service plan provides access to these services over a Wi-Fi network.

Types of Wi-Fi networks

Wi-Fi enabled BlackBerry devices can access BlackBerry services using enterprise Wi-Fi networks, home Wi-Fi networks, or hotspots.

Type	Description
Enterprise Wi-Fi networks	An enterprise Wi-Fi network has multiple wireless access points to provide ubiquitous coverage, hotspot coverage, or ubiquitous and hotspot coverage. You can use a Wi-Fi enabled BlackBerry device in any coverage area. You can configure an enterprise Wi-Fi network to require layer 2 authentication. An organization might consider an enterprise Wi-Fi network to be untrusted and require that all Wi-Fi connections to the organization's network occur through a VPN concentrator. You must configure Wi-Fi enabled BlackBerry devices to support the authentication type that your organization uses. An enterprise Wi-Fi network permits optimized access to the BlackBerry Enterprise Server over a direct IP connection to the BlackBerry Router.
Home Wi-Fi networks	A home Wi-Fi network uses a single access point to provide Internet access through a broadband gateway. The broadband gateway can implement NAT and

Type	Description
	permit VPN connections through the firewall. You can configure a home Wi-Fi network with layer 2 security and password authentication. You must configure BlackBerry devices to support the authentication that the home Wi-Fi network requires. A home Wi-Fi network permits users to access all BlackBerry services from Wi-Fi enabled BlackBerry devices using the BlackBerry Infrastructure.
Hotspots	A hotspot offered by an ISP, a mobile network provider, or a property owner can provide a Wi-Fi connection in public and semipublic areas. The network can be an open network without layer 2 security and use a captive portal for authentication. The captive portal blocks all network traffic except traffic that uses HTTP and it redirects HTTP requests to a login page. After a user logs in to the hotspot, the captive portal permits the user to access wireless network services. Hotspots can use a firewall and they can permit VPN connections. A hotspot permits users to access all BlackBerry services from their Wi-Fi enabled BlackBerry devices using the BlackBerry Infrastructure.

Security features of a Wi-Fi enabled device

Feature	Description
Activation of BlackBerry devices over an enterprise Wi-Fi network	Activation of devices over an enterprise Wi-Fi network is designed to simplify the actions of activating or updating devices.
Authenticated connection with BlackBerry Router	An authenticated connection with a BlackBerry Router permits devices to open a direct connection to the BlackBerry Enterprise Server after they authenticate with the BlackBerry Router. Devices connected to an enterprise Wi-Fi network do not use an SRP connection to send data to the BlackBerry Enterprise Server.
BlackBerry transport layer encryption	BlackBerry transport layer encryption is designed to encrypt messages that the device and the BlackBerry Enterprise Server send between each other after they open an authenticated connection.
Direct access to the BlackBerry Infrastructure over a Wi-Fi connection	Direct access to the BlackBerry Infrastructure over a Wi-Fi connection permits Wi-Fi enabled devices to access BlackBerry services over the Internet, even if UMA is not available.

Feature	Description
	You can verify with your organization's wireless service provider that your organization's service plan supports access to BlackBerry services over a Wi-Fi connection.
Encrypted communication over the Wi-Fi network	Devices support multiple security methods that are designed to encrypt communication over the enterprise Wi-Fi network between the device and wireless access points or a network firewall on the enterprise Wi-Fi network.
Expanded groups of Wi-Fi and VPN configuration settings	Expanded groups of Wi-Fi and VPN configuration settings permit you to control Wi-Fi connections from devices.
Limited connections	Wi-Fi enabled devices are designed to reject incoming connections, to support limited connections in infrastructure mode only, and to prevent ad-hoc mode (also known as peer-to-peer) connections.
Multiple Wi-Fi and VPN profiles	Multiple Wi-Fi and VPN profiles are designed to address user requirements in a variety of different environments.
Proxy server	Devices supports the use of a transparent proxy server that you can configure between the enterprise Wi-Fi network and the device.
Software token provisioning	Software token provisioning is designed to permit you to provision and manage the seed for software token authentication on devices. You can use software token authentication for VPN connections. The BlackBerry Enterprise Server is designed to work with the RSA Authentication Manager to provide software token support for use with layer 2 and layer 3 authentication on supported devices.
User-specific configuration settings and IT policy rules	User-specific configuration settings and IT policy rules are designed to simplify the configuration of user-specific Wi-Fi and VPN information (such as user IDs and passwords).
Wireless backup of Wi-Fi and VPN profiles	Backup of Wi-Fi and VPN profiles on devices over a Wi-Fi connection permits users to restore the profiles, if necessary.

Protecting a connection between a Wi-Fi enabled device and an enterprise Wi-Fi network

A Wi-Fi enabled BlackBerry device is designed to connect to enterprise Wi-Fi networks that use the IEEE® 802.11® standard. The IEEE 802.11i standard uses the IEEE 802.1X standard for authentication and key management to protect enterprise Wi-Fi networks. The IEEE 802.11i standard specifies that organizations must use the PSK protocol or the IEEE 802.1X standard as the access control methods for Wi-Fi networks.

When you configure a Wi-Fi enabled device to use an enterprise Wi-Fi network, you must configure the enterprise Wi-Fi network and device to protect all message data and application data that the BlackBerry Enterprise Server and device send to each other. For example, to help protect data, you can configure the device to authenticate with the enterprise Wi-Fi network before the device can access the enterprise Wi-Fi network. You can also configure the device and the enterprise Wi-Fi network to encrypt any communication that they send to each other.

For more information about protecting an enterprise Wi-Fi network, see the documentation from your organization's Wi-Fi solution provider.

How a Wi-Fi enabled device can connect to the BlackBerry Infrastructure

A Wi-Fi enabled BlackBerry device can connect directly to the BlackBerry Infrastructure over the Internet to access the data services that a wireless service provider offers, even if UMA is not available. If UMA is available, the device can also access the voice services. A direct connection from the device to the BlackBerry Infrastructure is an alternative to the connection from the device to the BlackBerry Infrastructure over the mobile network. If a user's wireless service provider makes UMA technology (also known as GAN technology) available, and the user subscribes to the UMA feature, the device is designed to open an SSL connection to the GANC using an IPSec VPN tunnel over an enterprise Wi-Fi network.

The device and BlackBerry Infrastructure send all data to each other over an SSL connection. The SSL connection is designed to encrypt the data that the device and BlackBerry Infrastructure send between each other.

How an SSL connection between a Wi-Fi enabled device and the BlackBerry Infrastructure protects data

An SSL connection between a Wi-Fi enabled BlackBerry device and the BlackBerry Infrastructure is designed to provide the same protection that an SRP connection between the BlackBerry Enterprise Server and BlackBerry Infrastructure provides. It is designed so that a potentially malicious user cannot use the SSL connection to send data to or receive data from the device.

If a potentially malicious user tries to impersonate the BlackBerry Infrastructure, the device is designed to prevent the connection. The device verifies whether the public key of the SSL certificate of the BlackBerry Infrastructure matches the private key of the root certificate that is preloaded on the device during the manufacturing process. If a user accepts a certificate that is not valid, the connection cannot open unless the device can also authenticate with a valid BlackBerry Enterprise Server or valid BlackBerry Internet Service.

Data flow: Opening an SSL connection between the BlackBerry Infrastructure and a Wi-Fi enabled device

1. A Wi-Fi enabled BlackBerry device sends a request to the BlackBerry Infrastructure to open an SSL connection.
2. The BlackBerry Infrastructure sends its SSL certificate to the device.
3. The device uses a root certificate that is preloaded on the device to verify the SSL certificate. If the user deleted the root certificate, the device prompts the user to trust the SSL certificate.
4. The device opens the SSL connection.

Cipher suites that a Wi-Fi enabled device supports for opening SSL connections and TLS connections

A Wi-Fi enabled BlackBerry device supports various cipher suites for direct mode SSL/TLS when the device opens SSL connections or TLS connections to the BlackBerry Infrastructure or to web servers that are external to your organization.

The device supports the following cipher suites, in order, when it opens SSL connections:

- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

The device supports the following cipher suites, in order, when it opens TLS connections:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DH_anon_WITH_AES_128_CBC_SHA
- TLS_DH_anon_WITH_AES_256_CBC_SHA
- TLS_DH_anon_WITH_RC4_128_MD5
- TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DHE_DSS_WITH_DES_CBC_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_EXPORT_WITH_RC4_40_MD5

- TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_DH_anon_WITH_DES_CBC_SHA
- TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA

Managing how a device connects to an enterprise Wi-Fi network

To manage how a Wi-Fi enabled BlackBerry device connects to an enterprise Wi-Fi network, you can use IT administration commands, IT policy rules, and configuration settings. You can turn on or turn off Wi-Fi access for the device in BlackBerry Enterprise Server version 4.1 SP3 or later, and manage Wi-Fi configuration settings and VPN configuration settings for user accounts in BlackBerry Enterprise Server version 4.1 SP2 or later.

When you configure an IT policy or configuration setting, a user cannot override the value on the device.

At an application level, you can specify the types of connections that an application can make. When you configure application control policies, you can control whether the application can access the enterprise Wi-Fi network.

For more information about specifying whether an application can access an enterprise Wi-Fi network, see *Protecting the BlackBerry Device Platform Against Malware*. For more information about using IT policy rules and configuration settings, see the *BlackBerry Enterprise Server Administration Guide* and the *BlackBerry Enterprise Server Policy Reference Guide* .

How the BlackBerry Enterprise Solution protects sensitive Wi-Fi information

To permit a Wi-Fi enabled BlackBerry device to access a Wi-Fi network, you must send sensitive Wi-Fi information such as encryption keys and passwords to the device using Wi-Fi profiles, VPN profiles, and IT policy rules. After the device receives the sensitive Wi-Fi information, the device encrypts the encryption keys and passwords and stores them in flash memory in an area that third-party applications cannot access.

The BlackBerry Enterprise Server encrypts the sensitive Wi-Fi information that it sends to the device and stores the sensitive Wi-Fi information in the BlackBerry Configuration Database. You can help protect the sensitive Wi-Fi information in the BlackBerry Configuration Database using access controls and configuration settings.

Using a VPN with a device

If your organization's environment includes VPNs, such as an IPSec VPN, you can configure a Wi-Fi enabled BlackBerry device to authenticate with the VPN so that it can access your organization's network. A VPN provides an encrypted tunnel between a device and your organization's network.

A VPN solution consists of a VPN client on the device and a VPN concentrator. The device can use the VPN client to authenticate with the VPN concentrator, which acts as the gateway to your organization's network. Each device includes a VPN client that supports several VPN concentrators. The VPN client on the device is designed to use strong encryption to authenticate with the VPN concentrator. It creates an encrypted tunnel between the device and VPN concentrator that the device and your organization's network can use to communicate.

After you configure the VPN, the device can use a layer 2 security method to connect to the enterprise Wi-Fi network, and use the VPN to authenticate with your organization's network. In this scenario, the enterprise Wi-Fi network is an untrusted network, and only the VPN can authenticate with your organization's network.

For a list of supported VPN concentrators, visit www.blackberry.com/support to read article KB13354.

Permitting a Wi-Fi enabled device to log in to a VPN concentrator

To permit a Wi-Fi enabled BlackBerry device to log in to a VPN concentrator automatically after it connects to an enterprise Wi-Fi network, you or a user can configure a VPN profile that includes a user name and password for authentication with the VPN concentrator. Depending on your organization's security policy, you or the user can save the user name and password for authentication with the VPN concentrator on the device. When you or the user saves the user name and password, the device does not prompt the user for the user name and password the first time or each time that the device connects to the enterprise Wi-Fi network.

The device is also compatible with VPN environments that use two-factor authentication using hardware tokens or software tokens for credentials. When the device tries to log in to the VPN, the device uses credentials that the token generates or that the user provides.

For more information about configuring VPN profiles, see the *BlackBerry Enterprise Server Administration Guide*.

Using a segmented network to reduce the spread of malware on an enterprise Wi-Fi network that uses a VPN

When a Wi-Fi enabled BlackBerry device connects to an enterprise Wi-Fi network that uses a VPN, the device might permit the VPN concentrator to send data directly to a BlackBerry Enterprise Server over your organization's network. The VPN concentrator sends data over port 4101. In this scenario, only the VPN concentrator connects to the enterprise Wi-Fi network.

To configure your organization's VPN concentrator to prevent it from opening unnecessary connections to your organization's network, you can configure a segmented network. In a segmented network, you can divide components of your organization's network using firewalls to reduce the spread of malware.

For more information about reducing the spread of malware, see *Protecting the BlackBerry device platform against malware*.

Supported UI settings for VPN concentrators

BlackBerry 7.1 supports the configuration of the following UI settings for the VPN concentrators that BlackBerry devices connect to.

UI setting	VPN-1 Power	Cisco VPN 3000 Series Concentrator			VPN Firewall Brick	NetScreen	Nortel Networks Contivity	Secure Computing Sidewinder	Symantec Raptor Firewall
Gateway Credential (PSK): Username (Group Name)	X	X	X	X	X	X	X	X	X
Gateway Credential (PSK): Password (Group Password)	X	X	X	X	X	X	X	X	X
XAuth Credential (PSK): Username		X	X	X	X	X	X	X	
XAuth Credential (PSK): Password		X	X	X	X	X	X	X	

UI setting	VPN-1 Power	Cisco VPN 3000 Series Concentrator			VPN Firewall Brick	NetScreen	Nortel Networks Contivity	Secure Computing Sidewinder	Symantec Raptor Firewall
XAuth Credential: Enable Extended Authentication			X		X	X	X		
Gateway Auth (PKI): Client Certificate		X	X			X	X		
Gateway Auth (PKI): CA Certificate		X	X			X	X		
DNS Config: Dynamically determine DNS		X	X	X	X		X	X	
External Network: Subnet IP address 1									X
External Network: Subnet mask 1									X
XAuth Credential: Extended Authentication							X		
IKE: DH Group	X	X	X	X	X	X	X	X	X
IKE: Cipher	X	X	X	X	X	X	X	X	X
IKE: Hash	X	X	X	X	X	X	X	X	X
IPSec: Perfect Forward Secrecy	X	X	X	X	X	X	X		X
IPSec: Crypto and Hash Suite	X	X	X	X	X	X	X	X	X
XAuth Credential: Soft Token			X	X					

Supported configurations for the Cisco VPN 3000 Series Concentrator

The following table describes the configurations that BlackBerry 7.1 supports for the Cisco VPN 3000 Series Concentrator.

Configuration setting	Configuration 1	Configuration 2	Configuration 3	Configuration 4
Gateway Credential (PSK): Username (Group Name)	X	X		
Gateway Credential (PSK): Password (Group Password)	X	X		
XAuth Credential (PSK): Username		X		X
XAuth Credential (PSK): Password		X		X
XAuth Credential: Enable Extended Authentication		X		X
Gateway Auth (PKI): Client Certificate			X	X
Gateway Auth (PKI): CA Certificate			X	X
DNS Config: Dynamically determine DNS	X	X	X	X
IKE: DH Group	Group 1	Group 1, 2	Group 5	Group 1, 5
IKE: Cipher	3DES, AES128	3DES, AES128	AES256	3DES, AES256
IKE: Hash	HMAC MD5, HMAC SHA1	HMAC MD5, HMAC SHA1	HMAC SHA1	HMAC MD5, HMAC SHA1
IPSec: Crypto and Hash Suite	3DES-MD5, AES128-SHA1	3DES-MD5, AES128-SHA1	AES256-SHA1	3DES-MD5, AES256-SHA1
NAT timeout	Default	Default	Default	Default

Supported configurations for the Cisco PIX Firewall

The following table describes the configurations that BlackBerry 7.1 supports for the Cisco PIX Firewall.

Configuration setting	Configuration 1	Configuration 2	Configuration 3	Configuration 4
Gateway Credential (PSK): Username (Group Name)	X	X		

Configuration setting	Configuration 1	Configuration 2	Configuration 3	Configuration 4
Gateway Credential (PSK): Password (Group Password)	X	X		
XAuth Credential (PSK): Username		X		X
XAuth Credential (PSK): Password		X		X
XAuth Credential: Enable Extended Authentication		X		X
Gateway Auth (PKI): Client Certificate			X	X
Gateway Auth (PKI): CA Certificate			X	X
DNS Config: Dynamically determine DNS	X	X	X	X
IKE: DH Group	Group 1, 2, 5	Group 1, 2, 5	Group 5	Group 5
IKE: Cipher	DES, 3DES, AES128, AES192, AES256	DES, 3DES, AES128, AES192, AES256	AES256	AES256
IKE: Hash	HMAC MD5, HMAC SHA1	HMAC MD5, HMAC SHA1	HMAC SHA1	HMAC SHA1
IPSec: Perfect Forward Secrecy				
IPSec: Crypto and Hash Suite	DES-SHA1, 3DES-MD5, 3DES-SHA1, AES128-MD5, AES128-SHA1, AES192-MD5, AES192-SHA1, AES256-MD5, AES256-SHA1	DES-SHA1, 3DES-MD5, 3DES-SHA1, AES128-MD5, AES128-SHA1, AES192-MD5, AES192-SHA1, AES256-MD5, AES256-SHA1	AES256-SHA1	AES256-SHA1
NAT timeout	Default	Default	Default	Default

Supported configurations for the Cisco IOS Easy VPN

The following table describes the configurations that the BlackBerry 7.1 supports for the Cisco IOS Easy VPN.

Configuration setting	Configuration 1	Configuration 2
Gateway Credential (PSK): Username (Group Name)	X	X

Configuration setting	Configuration 1	Configuration 2
Gateway Credential (PSK): Password (Group Password)	X	X
XAuth Credential (PSK): Username		X
XAuth Credential (PSK): Password		X
XAuth Credential: Enable Extended Authentication		X
DNS Config: Dynamically determine DNS	X	X
IKE: DH Group	Group 1	Group 1, 2, 5
IKE: Cipher	3DES	DES, 3DES, AES128, AES192, AES256
IKE: Hash	HMAC MD5	HMAC MD5, HMAC SHA1
IPSec: Crypto and Hash Suite	3DES-MD5	DES-SHA1, 3DES-SHA1, AES128-SHA1, AES192-SHA1, AES256-MD5, AES256-SHA1
NAT timeout	Default	Default

Supported configurations for the Secure Computing Sidewinder

The following table describes the configurations that BlackBerry 7.1 supports for the Secure Computing Sidewinder.

Configuration setting	Configuration 1
Gateway Credential (PSK): Username (Group Name)	X
Gateway Credential (PSK): Password (Group Password)	X
XAuth Credential (PSK): Username	X
XAuth Credential (PSK): Password	X
XAuth Credential: Enable Extended Authentication	X
DNS Config: Dynamically determine DNS	X
External Network: Subnet IP address 1	X
External Network: Subnet mask 1	X
IKE: DH Group	Group 1

Configuration setting	Configuration 1
IKE: Cipher	3DES
IKE: Hash	HMAC MD5
IPSec: Crypto and Hash Suite	3DES-MD5
NAT timeout	Default

Supported configurations for Nortel Networks Contivity

The following table describes the configurations that BlackBerry 7.1 supports for Nortel Networks Contivity.

Configuration setting	Configuration 1	Configuration 2
Gateway Credential (PSK): Username (Group Name)	X	X
Gateway Credential (PSK): Password (Group Password)	X	X
XAuth Credential (PSK): Username		X
XAuth Credential (PSK): Password		X
DNS Config: Dynamically determine DNS	X	X
XAuth Credential: Extended Authentication		X
IKE: DH Group	Group 1	Group 1
IKE: Cipher	3DES	3DES
IKE: Hash	HMAC MD5	HMAC MD5
IPSec: Crypto and Hash Suite	3DES-MD5	3DES-MD5
NAT timeout	Default	Default

Using a captive portal to connect to an enterprise Wi-Fi network or Wi-Fi hotspot

A captive portal uses web-based authentication to permit a Wi-Fi enabled BlackBerry device to connect to an enterprise Wi-Fi network or Wi-Fi hotspot. The BlackBerry device can use a captive portal to access an IP segment of the enterprise

Wi-Fi network or Wi-Fi hotspot. After the BlackBerry device connects to the enterprise Wi-Fi network or Wi-Fi hotspot, the user can browse to an HTML login page for a web site that permits the enterprise Wi-Fi network or Wi-Fi hotspot to authenticate with the BlackBerry device before the BlackBerry device can access the web site.

If your organization uses a captive portal, you can permit a user to access the captive portal using the WLAN Login browser on the BlackBerry device. The user must authenticate with the WLAN Login browser using the login information that you provide.

When the BlackBerry device authenticates with the captive portal, the user can use the BlackBerry Browser on the BlackBerry device to access other web sites and data services that are available on the enterprise Wi-Fi network or Wi-Fi hotspot.

Protecting a connection between a Wi-Fi enabled device and an enterprise Wi-Fi network using RSA SecurID

You can use software tokens to provide layer 2 authentication or layer 3 authentication on a Wi-Fi enabled BlackBerry device. When you configure a software token for a user, the device is designed to use the passcode to authenticate the user to the Wi-Fi network using PEAP authentication, EAP-GTC authentication, EAP-FAST authentication, EAP-TTLS authentication, or a VPN.

The RSA SecurID Library on the device permits the device to periodically generate token codes for a software token. The device imports a seed, which consists of random data, and uses the seed to initialize the software token algorithm. The software token algorithm generates token codes on the device.

An RSAadministrator can use RSA Authentication Manager 6.1 or later to configure an optional password to encrypt the seed. The RSA SecurID library on the device can decrypt the seed using the optional password. The RSA SecurID library uses code signing to help prevent third-party applications from changing or reading the information that the RSA SecurID library stores on the device.

When the user opens a Wi-Fi connection or VPN connection that requires two-factor authentication on the device, the device prompts the user to type the software token PIN. The RSA SecurID Library adds the software token PIN to the beginning of the current token code to create a passcode that the device uses in the two-factor authentication process.

BlackBerry transport layer encryption is designed to protect the seed when the BlackBerry Enterprise Server sends it over the transport layer. The device uses Research In Motion proprietary protocols that are designed to be highly secure to perform all communication necessary to retrieve the seed on behalf of the RSA SecurID Library.

Data flow: Generating a token code for a software token

1. An RSA administrator uses the RSA Authentication Manager to import a seed as a soft token file in .asc format to a software token database and issue the software token file in .sdtid format. If necessary, the administrator can perform one or more of the following actions:
   - Permit a user to specify the software token PIN
   - Configure the RSA SecurID to automatically generate and send a software token PIN to a Wi-Fi enabled BlackBerry device
   - Require the user to specify the software token PIN the first time that the user tries to complete RSA authentication on the device
   - Bind the seed to a specific device PIN
   - Specify an optional password to encrypt the .sdtid seed file
2. You assign the .sdtid file seed for the device to the user account in the BlackBerry Administration Service. If required, you specify the optional password that the device can use to decrypt the seed.
3. The BlackBerry Enterprise Server performs the following actions:
   a Stores the .sdtid seed file in the BlackBerry Configuration Database.
   b Pushes the .sdtid seed file (and the password, if the RSAadministrator specified one) to the device during the activation process and each time that the RSA administrator changes the .sdtid seed file for the device.
4. The device performs the following actions:
   a Imports the .sdtid seed file. If the RSA administrator specified a password in the RSA Authentication Manager to encrypt the .sdtid file seed, the device uses the password to decrypt the .sdtid seed file. If the RSA administrator specified that the .sdtid seed file must bind to a specific device PIN, only the device with the specific PIN can import the seed.
   b Stores the .sdtid seed file in flash memory.
   c Imports a copy of the .sdtid seed file into the RSA SecurID on the device.
5. The RSA SecurID randomly generates a password to encrypt the .sdtid seed file.
6. The RSA SecurID library on the device authenticates with the RSA Authentication Agent and initializes the software token algorithm one time for each minute.
7. Each time the user tries to open a Wi-Fi connection or VPN connection that requires RSA authentication, the device uses the initialized algorithm to combine the .sdtid file seed with random data that is based on the time and generate a new token code for the software token.

Layer 2 security methods that a device supports

You can configure a Wi-Fi enabled BlackBerry device to use security methods for layer 2 (also known as the IEEE 802.11 link layer) so that the device can authenticate with a wireless access point and the device and access point can encrypt data that they send between each other. The device supports the following layer 2 security methods:

- Open (no security method)
- WEP encryption (64-bit and 128-bit)
- IEEE 802.1X standard and EAP authentication using EAP-FAST, EAP-SIM, EAP-TLS, EAP-TTLS, LEAP, and PEAP

To support IEEE 802.1X methods, the device has a built-in supplicant.

The device also supports TKIP and AES-CCMP encryption for WPA-Personal, WPA2-Personal, WPA-Enterprise, and WPA2-Enterprise. When the device is roaming from one access point to another access point, the device supports the IEEE 802.11r standard that is included in the Wi-Fi CERTIFIED Voice-Enterprise program.

If your organization's enterprise Wi-Fi network uses EAP authentication, you can permit and deny device access to the enterprise Wi-Fi network by updating your organization's central authentication server. You are not required to update the configuration of each access point.

For more information about IEEE 802.11 and IEEE 802.1X, see www.ieee.org/portal/site. For more information about EAP authentication, see RFC 3748.

WEP encryption

WEP encryption uses a matching encryption key at a wireless access point and on a Wi-Fi enabled BlackBerry device to protect the connection to a Wi-Fi network. The encryption key can be 40 bits in length (for 64-bit WEP encryption) or 104 bits in length (for 128-bit WEP encryption). To configure a device to use WEP encryption, you must send WEP encryption keys to the device using IT policy rules or configuration settings.

By current industry standards, WEP encryption is not a cryptographically strong security solution. WEP encryption weaknesses include the following scenarios:

- A potentially malicious user might capture transmissions over the wireless network and might deduce WEP encryption keys in very little time.
- A potentially malicious user might use a man-in-the-middle attack to change packets that are encrypted using WEP encryption.

You can use a VPN to provide data confidentially if your organization uses WEP encryption. A VPN can authenticate and encrypt access to your organization's network.

For more information about configuring WEP encryption, see the *BlackBerry Enterprise Server Administration Guide*.

WPA authentication

The IEEE 802.1X standard specifies the WPA protocol as an access control method for work Wi-Fi networks. You can also use WPA authentication in small-office environments and home environments where you cannot configure server-based authentication.

To configure WPA authentication, you can use the PSK protocol to send a passphrase that matches the key or passphrase for the wireless access points to a Wi-Fi enabled BlackBerry device. The access points and device use a passphrase to generate layer 2 encryption keys. The passphrase can be up to 256 bits. All access points and each device in your organization must share the same passphrase.

The PSK protocol is designed to use TKIP keys or AES-CCMP keys to protect communications over the enterprise Wi-Fi network. The PSK protocol relies on the passphrase to control whether a device can access the work Wi-Fi network.

The device is compatible with the WPA-Personal specification and WPA2-Personal specification.

For more information about configuring the device to support WPA authentication, see the *BlackBerry Enterprise Server Administration Guide*.

IEEE 802.1X standard

18

The IEEE 802.1X standard defines a generic authentication framework that a Wi-Fi enabled BlackBerry device and an enterprise Wi-Fi network can use for authentication. The EAP framework that the IEEE 802.1X standard uses for authentication is specified in RFC3748.

The device supports EAP authentication methods that meet the requirements of RFC4017. The device uses the EAP authentication methods to authenticate with the enterprise Wi-Fi network. Some EAP authentication methods (for example, EAP-TLS, EAP-TTLS, EAP-FAST, or PEAP) use credentials to provide mutual authentication between the device and the enterprise Wi-Fi network.

The device is compatible with the WPA-Enterprise and WPA2-Enterprise specifications.

Roaming in an enterprise Wi-Fi network

The BlackBerry device is designed to minimize loss of network connectivity when it moves from one wireless access point to another in an enterprise Wi-Fi network that uses WPA2-Enterprise authentication. If the enterprise Wi-Fi network supports Wi-Fi CERTIFIED Voice-Enterprise, the device uses the IEEE 802.11r standard to move from one wireless access point to another. If the enterprise Wi-Fi network does not use Wi-Fi CERTIFIED Voice- Enterprise, the device uses the IEEE 802.11i standard with the IEEE 802.1X standard to move from one wireless access point to another.

When the device uses the IEEE 802.11i standard with the IEEE 802.1X standard, the key exchange that occurs during EAP authentication generates the required keying material. The device and a wireless access point use the keying material when they create the PMK.

The device and wireless access point can cache the PMK. The PMK caching process permits the device and the access point to generate session keys and skip EAP authentication during subsequent connections. PMK caching helps reduce the roaming latency for the device when the device moves to another access point in an enterprise Wi-Fi network.

Data flow: Authenticating a Wi-Fi enabled device with a work Wi-Fi network using the IEEE 802.1X standard

If you configured a wireless access point to use the IEEE 802.1X standard, the access point permits communication using EAP authentication only. This process flow assumes that you configured a Wi-Fi enabled BlackBerry device to use an EAP authentication method to communicate with the access point.

1. The Wi-Fi enabled device associates itself with the access point that you configured to use the IEEE 802.1X standard. The device sends its credentials (typically a user name and password) to the access point.
2. The access point sends the credentials to the authentication server.
3. The authentication server performs the following actions:
   a authenticates the device on behalf of the access point
   b instructs the access point to permit access to the work Wi-Fi network
   c sends Wi-Fi credentials to the device to permit it to authenticate with the access point
4. The access point and device use EAPoL-Key messages to generate encryption keys (for example, WEP, TKIP, or AES-CCMP, depending on the EAP authentication method that the device uses).

   When the device sends EAPoL messages, the device uses the encryption and integrity requirements that the EAP authentication method specifies. When the device sends EAPoL-Key messages, the device uses the ARC4 algorithm or AES algorithm to provide integrity and encryption.

After the access point and device generate the encryption key, the device can access the work Wi-Fi network.

EAP authentication methods that a Wi-Fi enabled device supports

LEAP authentication

LEAP authentication is designed to improve WEP authentication. You can use LEAP authentication to authenticate a Wi-Fi enabled BlackBerry device with a work Wi-Fi network, generate WEP encryption keys that are unique to the device, and configure the work Wi-Fi network to update the WEP encryption keys automatically during a session with the device.

The device supports using LEAP authentication with a user name and password. The device uses a one-way function to encrypt the password before it sends the password to the authentication server on the work Wi-Fi network. You can configure password policies on a work Wi-Fi network that require the device to use LEAP authentication to connect to the work Wi-Fi network.

LEAP authentication does not provide mutual authentication between the device and work Wi-Fi network.

PEAP authentication

PEAP authentication permits a Wi-Fi enabled BlackBerry device to authenticate with an authentication server and access a work Wi-Fi network. PEAP authentication uses TLS to create an encrypted tunnel between the device and the authentication server. The device uses the TLS tunnel to send the authentication credentials to the authentication server.

The device supports PEAPv0 and PEAPv1 for PEAP authentication. The device also supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during PEAP authentication. The device can use the second-phase protocols to exchange credentials with the work Wi-Fi network.

To configure PEAP authentication, you must install a root certificate on the device that corresponds with the authentication server certificate and install client certificates, if required.

For more information, see the *BlackBerry Enterprise Server Administration Guide.*

EAP-TLS authentication

EAP-TLS authentication uses a PKI to permit a Wi-Fi enabled BlackBerry device to authenticate with an authentication server and access a work Wi-Fi network. EAP-TLS authentication uses TLS to create an encrypted tunnel between the device and the authentication server. EAP-TLS authentication uses the TLS encrypted tunnel and a client certificate to send the credentials of the device to the authentication server.

The device supports EAP-TLS authentication when the authentication server and client use certificates that meet specific requirements for authentication. To configure EAP-TLS authentication, you must install a client certificate and a root certificate on the device that corresponds to the certificate of the authentication server. For more information, see the *BlackBerry Enterprise Server Administration Guide*.

For more information about EAP-TLS authentication, see RFC 2716.

EAP-TTLS authentication

EAP-TTLS authentication extends EAP-TLS authentication to permit a Wi-Fi enabled BlackBerry device and an authentication server to authenticate with each other. When the authentication server uses its certificate to authenticate with the device and open a protected connection to the device, the authentication server uses an authentication protocol over the protected connection to authenticate the device.

The device supports EAP-MS-CHAPv2 and MS-CHAPv2 as second-phase protocols during EAP-TTLS authentication so that the device can exchange credentials with the work Wi-Fi network.

To configure EAP-TTLS authentication, you must install the root certificate on the device that corresponds to the certificate of the authentication server. For more information, see the *BlackBerry Enterprise Server Administration Guide*.

EAP-FAST authentication

EAP-FAST authentication uses PAC to open a TLS connection to a Wi-Fi enabled BlackBerry device and verify the supplicant credentials of the device over the TLS connection.

The device supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during EAP-FAST authentication so that the device can exchange authentication credentials with the work Wi-Fi network. The device supports using automatic PAC provisioning with EAP-FAST authentication only.

For more information about EAP-FAST authentication, see RFC 4851.

EAP-SIM authentication

EAP-SIM authentication uses a GSM SIM card to authenticate a Wi-Fi enabled BlackBerry device with a work Wi-Fi network and distribute session keys. EAP-SIM authentication uses a challenge-response method without mutual authentication.

The device supports using EAP-SIM authentication with the credentials on the GSM SIM card only. The user is not required to type or select credentials on the device.

The user identity that EAP-SIM uses for authentication on the device is built from IMSI using the 3GPP technical specification 3GPP-TS-23.003.

The device can receive at least two challenges from the authentication server to provide stronger authentication.

For more information about EAP-SIM authentication, see RFC 4186.

Encryption keys that a Wi-Fi enabled device supports for use with layer 2 security methods

A Wi-Fi enabled BlackBerry device supports AES-CCMP encryption keys, TKIP encryption keys, and WEP encryption keys.

The device supports the use of AES-CCMP with the following authentication methods:

- EAP-FAST authentication
- EAP-TLS authentication
- EAP-TTLS authentication
- PEAP authentication
- PSK authentication

The device supports the use of TKIP with the following authentication methods:

- EAP-FAST authentication
- EAP-TLS authentication
- EAP-TTLS authentication
- PEAP authentication
- PSK authentication

For more information about AES-CCMP and TKIP, visit www.ieee.org/portal/site.

Support for the use of CCKM with EAP authentication methods

A Wi-Fi enabled BlackBerry device supports the use of CCKM with all supported EAP authentication methods to improve roaming between wireless access points. The device does not support the use of CCKM with the Cisco CKIP encryption algorithm or the AES-CCMP encryption algorithm.

Using certificates with PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication

If your organization uses PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to protect the wireless access points for your organization's work Wi-Fi network, a Wi-Fi enabled BlackBerry device must authenticate mutually with an access point using an authentication server. To generate the certificates that the device and authentication server use to authenticate with each other, you require a certification authority.

For PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to be successful, the device must trust the certificate of the authentication server. The device does not trust the certificate of the authentication server automatically. Before you can configure the device to trust the certificate of the authentication server, the following conditions must exist:

- A certification authority that the device and authentication server mutually trust must generate the certificate of the authentication server and a certificate for the device.
- The device must store the root certificates in the certificate chain for the certificate of the authentication server.

Each device stores a list of root certificates that are issued by certification authorities that it trusts.

Controlling applications on a device

19

Creating an application for a smartphone

An application developer can create an application for BlackBerry smartphones using a variety of developer tools.

Applications can perform the following actions on a smartphone:

- Share application data with other applications
- Access user data such as calendar entries, email messages, and contacts
- Control smartphone resources, such as the camera or GPS

Some applications are preloaded on smartphones. You can use the BlackBerry Administration Service to install and manage applications on smartphones. A user can also download and install applications on a smartphone using a computer or over the wireless network.

For more information on the tools available for application developers, visit www.blackberry.com/developers .

Specifying the methods that users can use to install applications on a smartphone

BlackBerry smartphone users can install applications using the following methods:

- Using the BlackBerry App World storefront
- Using a browser
- Using a media card
- Over a USB connection (for example, using the BlackBerry Desktop Software or BlackBerry Application Web Loader)

You can use the Application Installation Methods IT policy rule to specify which application installation options are available to a user. You can also use the Installation from Specified URLs Only IT policy rule to specify a list of web addresses that a user can download applications from.

For more information about using IT policy rules, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Enterprise Server Policy Reference Guide*.

Specifying the resources that applications can access on a device

You can specify which applications a BlackBerry device user can download and install on a BlackBerry device and the resources on the device that the applications can access. If you control the applications that a user can install and limit the resources that the applications can access, you can help protect the device from malware. You can also help prevent damage to the device, applications, device data, and your organization's network.

You can use application control policy rules and code signing to control the resources that applications can access on devices and to help prevent malware on devices.

For more information about helping to prevent malware on devices, see *Protecting Devices From Malware*.

Using application control policy rules to control the resources that applications can access on a smartphone

You can use application control policy rules to specify whether users can install applications on BlackBerry smartphones and to specify the permissions for applications.

You can use application control policy rules to specify whether applications can access the following resources on smartphones:

- Data or applications (for example, Messages application, phone)
- Smartphone key store
- Network connections
- Near field communications
- Secure element
- Smartphone settings
- Security timer
- BlackBerry APIs (for example, GPS API, User Authenticator API, Module Management API)

When you assign an application control policy to a software configuration and assign the software configuration to user accounts or groups, users might not be able to use all of the features of the applications that are included in the software configuration. For example, if you set the "Are External Network Connections Allowed" application control policy rule to

"Not permitted", a game that is installed on a smartphone may not be able to send high scores back to a central server since the game is not permitted to access the Internet.

You can assign application control policies to software configurations so that the BlackBerry Enterprise Server limits the permitted application behavior to a subset of user accounts that it trusts.

Smartphones revoke the application control policy and reset if the permissions for applications that the application control policy is applied to become more restrictive. Smartphones permit users to make application permissions more restrictive, but never less restrictive, than the permissions that you specify.

For more information about configuring application control policies, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Enterprise Server Administration Guide*.

Application permissions for applications that users install on a smartphone

Users can set permissions that control how applications that users install on a BlackBerry smartphone interact with the other applications on the smartphone. For example, a user can control whether an application that the user installs on the smartphone can access data or the Internet, make calls, or use Bluetooth connections.

If a user adds an application to the smartphone, the smartphone is designed to prevent the application from sending or receiving data without the user's knowledge. For a selected application or all your third-party applications, before an application sends or receives data, you can turn on a prompt that allows you to accept or deny the connection request for a specific location or resource.

Smartphones permit users to make application permissions more restrictive, but never less restrictive, than the permissions that you specify.

The following table shows the application permissions and their default settings:

Permission	Category	Default setting	Description
USB	Connections	Allow	A user can set whether applications can use physical connections, such as a USB cable, that a user set up for the smartphone.
Bluetooth	Connections	Allow	A user can set whether applications can use Bluetooth connections.
Phone	Connections	Prompt	A user can set whether applications can make calls or access call logs.
Location Data	Connections	Prompt	A user can set whether applications can use the GPS location information on the smartphone.
Server Network	Connections	• Allow (BlackBerry 7 and later)	A user can set whether applications can access the Internet or your organization's intranet using your organization's network.

Permission	Category	Default setting	Description
		• Prompt (BlackBerry Device Software 6.0 and earlier)	
Internet	Connections	• Allow (BlackBerry 7 and later) • Prompt (BlackBerry Device Software 6.0 and earlier)	A user can set whether applications can access the Internet through a wireless service provider (for example, using a direct Internet connection or WAP gateway).
Wi-Fi	Connections	Allow	A user can set whether applications can use Wi-Fi connections.
Near Field Communication	Connections	Allow	A user can set whether applications can use NFC connections.
Cross Applications Communication	Interactions	Allow	A user can set whether applications can communicate and share data with other applications on the smartphone.
Device Settings	Interactions	Allow	A user can set whether applications can turn on or turn off the smartphone or change smartphone options, such as display options.
Media	Interactions	Allow	A user can set whether applications can access media files on the smartphone.
Application Management	Interactions	Allow	A user can set whether applications can add or delete application modules or access module information such as an application name or version.
Themes	Interactions	Allow	A user can set whether the smartphone can use applications as a source for customized themes.
Input Simulation	Interactions	Deny	A user can set whether applications can simulate actions, such as pressing a key on the smartphone.
Browser Filtering	Interactions	Deny	A user can set whether applications can register browser filters with the browser on the smartphone to add, change, or delete website content before it appears in the browser.

Permission	Category	Default setting	Description
Recording	Interactions	Prompt	A user can set whether applications can take screen shots of the smartphone screen or use other applications on the smartphone to take pictures or recordings.
Security Timer Reset	Interactions	Deny	A user can set whether applications can reset the duration that the smartphone remains unlocked after the user stops using it.
Display Information While Locked	Interactions	Deny	A user can set whether applications can display information while the smartphone is locked.
Email	User Data	Allow	A user can set whether applications can access email messages, SMS text messages, MMS messages, or PIN messages on the smartphone.
Organizer Data	User Data	Allow	A user can set whether applications can access organizer data such as contacts, calendar entries, tasks, or memos on the smartphone.
Files	User Data	Allow	A user can set whether applications can access files that the user stores on the smartphone. For example, a user can set whether applications can access files that a user transfers to the smartphone using the media manager tool of the BlackBerry Device Software or Bluetooth technology.
Security Data	User Data	Allow	A user can set whether applications can access certificates or keys in the key store on the smartphone.
Secure Element	User Data	Allow	A user can set whether applications can access confidential information, such as credit card numbers, coupons, loyalty cards, and public transit passes, that are stored on the smartphone's secure element. Depending on the smartphone model and wireless service provider, the smartphone might not use a secure element.

Application permissions for applications that users install as trusted applications on a smartphone

Some applications that a user installs on a BlackBerry smartphone prompt the user to install the application as a trusted application. If the user accepts the prompt and installs the application as a trusted application, all permissions for the application are set to Allow except for the following permissions:

Permission	Setting
Input Simulation	Deny
Browser Filtering	Deny
Recording	Prompt
Security Timer Reset	Prompt
Display Information While Locked	Deny
Secure Element	Prompt

How code signing controls the resources that applications can access on a smartphone

Some APIs in the BlackBerry Java SDK are protected APIs. Protected APIs expose methods that can access user data or other information on BlackBerry smartphones that is considered sensitive. When an application uses protected APIs, the application must be digitally signed with code signing keys before the application can be deployed.

Application developers can request access to a set of code signing keys from blackberry.com/SignedKeys/. The developer must digitally sign the application before it can be installed on a smartphone. Code signing does not certify or approve an application, but it allows Research In Motion to identify the author of a potentially malicious application that uses sensitive APIs.

In addition to API control, code signing can be used to restrict or share access to application data by other applications on a smartphone.

For more information about code signing and applications, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Java SDK Security Development Guide*.

Permitting an application to encode data on a smartphone

A developer can use the Transcoder API to create an encoding scheme for data that a BlackBerry Enterprise Server and BlackBerry smartphone send between each other. The Transcoder API is part of the BlackBerry Java SDK. The BlackBerry Enterprise Server and the smartphone can use the encoding scheme to encode and decode all gateway message envelope packets that the BlackBerry Enterprise Server and the smartphone send between each other. The encoding scheme adds a transcoder ID to the beginning of the encoded data.

By default, the BlackBerry Enterprise Solution encrypts the encoded data using BlackBerry transport layer encryption. If the Primary Transcoder IT policy rule specifies that the transcoder is outside, the data is encrypted using BlackBerry transport layer encryption first, and then encoded by the transcoder if both the BlackBerry Enterprise Server and the smartphone support it.

Before an application can access the Transcoder API, the BlackBerry Signing Authority Tool must digitally sign the .cod file. The BlackBerry Signing Authority Tool uses the code signing keys to authorize and authenticate the Transcoder implementation code.

To permit the BlackBerry Enterprise Server and the smartphone to use the encoding scheme, you must specify the hash of the application's .cod file in the Security Transcoder Cod File Hashes IT policy rule. To use the transcoder to encode the data after BlackBerry transport layer encryption is applied, you must also set the Primary Transcoder IT policy rule.

If the RIM Cryptographic API does not support a specific algorithm, the developer can use the Transcoder API to add the algorithm to the encoding schemes. The BlackBerry Enterprise Solution applies the encoding schemes to any outgoing data that the BlackBerry transport layer encryption applies to. By default, the Transcoder API supports all algorithms that the RIM Cryptographic API supports.

If you permit applications to use the Transcoder API on the smartphone, the applications might impact the security, usability, and performance of the BlackBerry Enterprise Solution. It might also cause the smartphone to lose data.

Removing applications that a user installed when a user deletes all smartphone data

If a user clicks Security Wipe in the security options on a BlackBerry smartphone, the user can select the User Installed Applications option at the same time. If the user selects this option, when the smartphone permanently deletes user data, it also removes all applications that a user installed on the smartphone, along with the application data.

Removing add-on applications from a device

You can create a software configuration to remove all add-on applications that are preloaded on a BlackBerry device. You can create an allowed list of applications by creating a software configuration and setting the disposition for unlisted applications to Disallowed. This removes all add-on applications developed by RIM and any third-party applications that you do not list as Required or Optional within the software configuration.

You can also create a custom software configuration to remove one or more add-on applications that are preloaded on a device but allow other add-on applications to remain on the device. To remove specific applications, you must add them to the application repository, then add them to the software configuration, and set the disposition for them to Disallowed. After you associate the software configuration to a group, multiple user accounts, or a single user account, the applications are removed from the device and the user cannot reinstall them.

The specific version of the application that you are removing must be included in the software configuration; versions other than the one you specify (for example, earlier and later versions) are not removed.

Users can also remove add-on applications that are preloaded on the device by deleting them from the application list on the device.

For more information about how to control third-party applications and add-on applications and how to remove third-party applications and add-on applications from a device, visit www.blackberry.com/support to read KB05392. For more information about which applications are add-on applications developed by RIM, visit www.blackberry.com/support to read KB24317.

Controlling which applications can access NFC features on a device

NFC technology is a short-range, wireless technology that is designed to allow BlackBerry device users to quickly exchange information between their BlackBerry devices and smart accessories, smart payment terminals, and smart tags.

You can use the "Is Access to NFC Allowed" application control policy rule to control which applications on the device can access NFC features. The NFC features on the device are tag reading, tag writing, and card emulation. This rule includes one of the following values:

- Allow: the application is permitted to access the NFC features on the device. The user can set the Near Field Communication permission to Allow, Prompt, or Deny in the Application Management options on the device.
- Not permitted: the application is not allowed to access the NFC features on the device. The user can only set the Near Field Communication permission to Deny in the Application Management options on the device.

- Prompt user: the device displays a message that provides the user with the option to Allow or Deny the application's request to access NFC features on the device. The user can set the Near Field Communication permission to Prompt or Deny in the Application Management options on the device.

For descriptions of application control policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*. For more information about configuring application control policy rules, see the *BlackBerry Enterprise Server Administration Guide*.

Controlling which applications can access the secure element on a device

You can use the "Is Access to the Secure Element Allowed" application control policy rule to control which applications on the BlackBerry device can access the secure element. The secure element stores information, such as credit card information and identification, so that the device can use NFC features. This rule includes the following values:

- Allow: the application is permitted to access the secure element on the device. The BlackBerry device user can set the Secure Element permission to Allow, Prompt, or Deny in the Application Management options on the device.
- Not permitted: the application is not allowed to access the secure element on the device. The user can only set the Secure Element permission to Deny in the Application Management options on the device.
- Prompt user: the device displays a message that provides the user with the option to Allow or Deny the application's request to access the secure element on the device. The user can set the Secure Element permission to Prompt or Deny in the Application Management options on the device.

For descriptions of application control policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*. For more information about configuring application control policy rules, see the *BlackBerry Enterprise Server Administration Guide*.

RIM Cryptographic API

20

The RIM Cryptographic API that is on a BlackBerry device and in the BlackBerry Java Development Environment consists of a Java interface that includes an encryption algorithm, a key agreement scheme, a signature scheme algorithm, a key generation algorithm, a message authentication code, cipher suites, a message digest, and a hash code.

A developer can use the BlackBerry JDE to access the RIM Cryptographic API to create an application that can run on the device. The developer is not required to change or access the encryption code directly because all calls to the native C++ encryption code are sent through the Java code.

Research In Motion uses code signing to authorize and authenticate an application and permit it to run on the device. Code signing is also used to control the ability of the application to access the RIM Cryptographic API.

Cryptographic algorithms and cryptographic codes that the RIM Cryptographic API supports

Symmetric block algorithms that the RIM Cryptographic API supports

Symmetric block algorithms use PKCS #5 for padding. The RIM Cryptographic API supports the CBC, CFB, ECB, OFB, and X modes for all algorithms. The RIM Cryptographic API implements the modes separately from the symmetric block algorithms.

Algorithm	Key length (bits)
AES	128, 192, and 256
CAST5	128
DES	56
RC2	8 to 1024

Algorithm	Key length (bits)
RC5	0 to 2040
Skipjack	80
Triple DES	112 and 168

Stream encryption algorithms that the RIM Cryptographic API supports

The RIM Cryptographic API supports the ARC4 algorithm, with an unlimited key length, as the symmetric stream encryption algorithm.

The RIM Cryptographic API supports the ECIES algorithm, with an unlimited key length (160 bits to 571 bits for seeding), as the asymmetric stream encryption algorithm.

Asymmetric encryption algorithms that the RIM Cryptographic API supports

Algorithm	Key length (bits)	Type
ElGamal	512 to 4096	discrete logarithm
RSA raw	512 to 4096	integer factorization
RSA with OAEP formatting	512 to 4096	integer factorization
RSA with PKCS #1 formatting (versions 1.5 and 2.0)	512 to 4096	integer factorization

Key agreement scheme algorithms that the RIM Cryptographic API supports

Algorithm	Key length (bits)	Type
Diffie-Hellman	512 to 4096	discrete logarithm

Algorithm	Key length (bits)	Type
ECDH	160 to 571	(Elliptic Curve) discrete logarithm
ECMQV	160 to 571	(Elliptic Curve) discrete logarithm
KEA	1024	discrete logarithm

Signature scheme algorithms that the RIM Cryptographic API supports

If the signature scheme algorithm that a developer wants to use is the RSA algorithm using ANSI X9.31, ANSI X9.31 uses one of the following algorithms for the required message digest code: SHA-1, SHA-2, or RIPEMD-160.

Algorithm	Key length (bits)	Type
DSA	512 to 1024	discrete logarithm
ECDSA	160 to 571	(Elliptic Curve) discrete logarithm
ECNR	160 to 571	(Elliptic Curve) discrete logarithm
RSA using ANSI X9.31	512 to 4096	integer factorization
RSA using PKCS #1 (versions 1.5 and 2.0)	512 to 4096	integer factorization
RSA using PSS	512 to 4096	integer factorization

Key generation algorithms that the RIM Cryptographic API supports

Algorithm	Key length (bits)	Type
Diffie-Hellman	512 to 4096	discrete logarithm
DSA	512 to 1024	discrete logarithm
Elliptic Curve	160 to 571	(Elliptic Curve) discrete logarithm
RSA	512 to 2048	integer factorization

Message authentication codes that the RIM Cryptographic API supports

Code	Key length (bits)
CBC-MAC	variable (block cipher key length)
HMAC	variable

Message digest codes that the RIM Cryptographic API supports

Code	Digest length (bits)
MD2	128
MD4	128
MD5	128
RIPEMD	128, 160
SHA	160, 224, 256, 384, 512

TLS and WTLS protocols that the RIM Cryptographic API supports

The RIM Cryptographic API supports the cipher suite components for the TLS protocol and WTLS protocol that apply only to direct mode SSL/TLS and WTLS.

Cipher suites for the key establishment algorithm that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
DH_anon	DH_anon	RSA _768, DH_anon, DH_anon_512, DH_anon_768
DH_anon_EXPORT	DH_anon_EXPORT	RSA_anon_512
DHE_DSS	DHE_DSS	RSA_512
DHE_DSS_EXPORT	DHE_DSS_EXPORT	RSA_anon_768
RSA	RSA	RSA
RSA_EXPORT	RSA_EXPORT	RSA_anon

Symmetric algorithms that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
DES	ARC4-128	RC5® -64
DES-40		RC5-56
ARC4-128	DES	RC5-128
ARC4-128	Triple DES	DES-40
ARC4-128	AES-128	DES
ARC4-128	AES-256	Triple DES
ARC4-40	ARC4-40	RC5-40
Triple DES	DES-40	RC5

Hash algorithms that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
MD5	MD5	SHA
SHA-1	SHA-1	SHA-40, SHA-80, MD5, MD5-40, MD5-80

Limitations of RIM Cryptographic API support for cipher suites for the key establishment algorithm

The RIM Cryptographic API implementation of the TLS protocol and WTLS protocol supports the use of the RSA public key algorithm, DSA public key algorithm, and Diffie-Hellman key exchange algorithm, with the following limitations.

Cipher suite type	Typical component limitation
export	RSA and Diffie-Hellman: 1024 bytes or less
non-export	non elliptic curve operations: 4096 bytes

Limitations to non-export cipher suite types are due to the computational constraints of a BlackBerry device.

Related resources

21

Resource	Information
BlackBerry Enterprise Server Feature and Technical Overview	• understanding BlackBerry Enterprise Server architecture
BlackBerry Enterprise Server Installation Guide	• understanding system requirements • performing preinstallation tasks • installing the BlackBerry Enterprise Server
BlackBerry Enterprise Server Administration Guide	• generating and changing device transport keys • configuring extended messaging encryption • managing security • protecting lost or stolen BlackBerry devices
BlackBerry Enterprise Server Policy Reference Guide	• understanding BlackBerry Enterprise Server IT policy rules and application control policy rules • using IT policies and application control policies
BlackBerry Signing Authority Tool Administrator Guide	• understanding the BlackBerry Signing Authority Tool implementation of public key cryptography • installing, configuring, and managing the BlackBerry Signing Authority Tool • restricting access to APIs
BlackBerry Java Development Environment Fundamentals Guide	• understanding BlackBerry APIs in the BlackBerry Java Development Environment • understanding APIs, classes, and methods with limited access • retrieving custom IT policy rules from the IT policy API • installing applications using the BlackBerry Desktop Software • publishing applications over the wireless network

Resource	Information
BlackBerry Java Development Environment Development Guide	• using controlled APIs • using code signatures
BlackBerry Smart Card Reader Security Technical Overview	• understanding highly secure pairings between the device and BlackBerry Smart Card Reader • understanding how the initial key establishment protocol works • understanding how the connection key establishment protocol works
Enforcing Encryption of Internal and External File Systems on BlackBerry Devices Technical Overview	• understanding which data items devices encrypt by default • using encryption to protect stored files in the on-board device memory and media cards
Erasing File Systems on BlackBerry Devices Technical Overview	• understanding which data items are deleted from device memory when you or a user deletes the device memory • understanding the different methods of permanently deleting device memory
PGP Support Package for BlackBerry Devices Security Technical Overview	• understanding PGP security and encryption • using PGP Universal Server to store and manage PGP keys • searching for and validating PGP keys • sending and receiving PGP messages
Protecting the BlackBerry Device Platform Against Malware	• understanding the default behavior of the device • understanding malware vulnerabilities on the device • managing the risk of malware attacks • using IT policy rules, application control rules, and code signing to help contain malware on the device
S/MIME Support Package for BlackBerry Devices Technical Overview	• understanding S/MIME security and encryption • managing S/MIME certificates on the device and a computer
Security for BlackBerry Devices with Bluetooth Wireless Technology	• Bluetooth wireless technology overview • using and protecting Bluetooth enabled devices

Resource	Information
	• risks of using Bluetooth wireless technology on mobile devices
www.blackberry.com/security	• understanding BlackBerry Enterprise Solution security

Glossary

22

3GPP	Third Generation Partnership Project
Advanced Security SD card	An Advanced Security SD card is a media card that complies with the Advanced Security SD Extension Specification that the SD Association developed. BlackBerry devices support only microSD cards that use the MCEX security system.
AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard Counter Mode CBCMAC Protocol
ANSI	American National Standards Institute
API	application programming interface
ARC4	Alleged Rivest's Cipher 4
ASCII	American Standard Code for Information Interchange
BlackBerry device key	The BlackBerry device key is a randomly generated key that a BlackBerry device uses to encrypt data on media cards.
BlackBerry device key store	The BlackBerry device key store stores certificates, key pairs, and PGP keys that a BlackBerry device can use to help protect messages, access web sites, and connect to an enterprise Wi-Fi network. To access the items in the key store, the user must type a key store password.
BlackBerry device memory	The BlackBerry device memory consists of the NV store, flash memory, RAM, on-board device memory, and BlackBerry device key store.
BlackBerry inter-process protocol	The BlackBerry inter-process protocol is a BlackBerry proprietary protocol that generates the session key that BlackBerry Enterprise Solution components, such as the BlackBerry Enterprise Server and BlackBerry Mobile Voice System, can use to communicate in a highly securely manner with each other. The BlackBerry inter-process protocol generates the session key based on the communication password.
BlackBerry inter-process protocol encryption	BlackBerry inter-process protocol encryption encrypts communication between BlackBerry Enterprise Solution components to prevent other parties from viewing the data that the components send between each other.
BlackBerry MDS	BlackBerry Mobile Data System
BlackBerry MDS security protocol	The BlackBerry MDS security protocol is a BlackBerry proprietary protocol that helps protect the data that a BlackBerry device and the BlackBerry MDS Connection Service send between each other.

BlackBerry MVS	BlackBerry Mobile Voice System
BlackBerry transport layer encryption	BlackBerry transport layer encryption (formerly known as standard BlackBerry encryption) uses a symmetric key encryption algorithm to help protect data that is in transit between a BlackBerry device and the BlackBerry® Enterprise Server when the data is outside an organization's firewall.
CA	certification authority
CAC	Common Access Card
CAST	Carlisle Adams Stafford Tavares
CBC	cipher block chaining
CCKM	Cisco Centralized Key Management
CFB	cipher feedback
CHAP	Challenge Handshake Authentication Protocol
CKIP	Cisco Key Integrity Protocol
CLDC	Connected Limited Device Configuration
code-signing keys	Code-signing keys are the keys that are stored on media cards that sign files so that a user can install and run the files on a BlackBerry device.
communication password	The communication password is a password that BlackBerry Enterprise Solution components use for the BlackBerry inter-process protocol. The communication password is designed to prevent a potentially malicious user from viewing the data that the components send to each other.
content protection	Content protection helps protect user data on a locked BlackBerry device by encrypting the user data using the content protection key and ECC private key.
content protection key	The content protection key encrypts user data on a BlackBerry device when the device is locked.
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
device transport key	The device transport key (formerly known as the master encryption key) is unique to a BlackBerry device. The BlackBerry device and BlackBerry Enterprise Server use the device transport key to encrypt the message keys.
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DoS	denial of service
DNS	Domain Name System
DPA	Differential Power Analysis

DRBG	deterministic random bit generator
DSA	Digital Signature Algorithm
DSML	Directory Service Markup Language
DSML-enabled server	A BlackBerry device uses a DSML-enabled server to search for and download certificates.
DSS	Digital Signature Standard
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
EAP-FAST	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling
EAP-GTC	Extensible Authentication Protocol Generic Token Card
EAP-MS-CHAP	Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol
EAP-SIM	Extensible Authentication Protocol Subscriber Identity Module
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol Tunneled Transport Layer Security
ECB	electronic code book
ECC	Elliptic Curve Cryptography
ECC private key	The ECC private key decrypts the data that a BlackBerry device received when the BlackBerry device was locked.
ECC public key	The ECC public key encrypts the data that a BlackBerry device receives when the BlackBerry device is locked.
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Standard
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
ECNR	Elliptic Curve Nyberg Rueppel
EDE	Encryption-Decryption-Encryption
EDGE	Enhanced Data Rates for Global Evolution
Enterprise Service Policy	The Enterprise Service Policy controls which BlackBerry devices can connect to a BlackBerry Enterprise Server.
ephemeral key	The ephemeral key encrypts the ECC public key, ECC private key, and content protection key.
FIPS	Federal Information Processing Standards

flash memory	The flash memory is an internal file system on a BlackBerry device that stores application data and user data.
GAN	generic access network
GANC	generic access network controller
global PIN encryption key	The global PIN encryption key is a key that is added to all BlackBerry devices during the manufacturing process. The global PIN encryption key permits devices to encrypt, decrypt, and authenticate PIN messages that are exchanged between devices.
gateway message envelope	The gateway message envelope protocol is a Research In Motion proprietary protocol that allows the transfer of compressed and encrypted data between the wireless network and BlackBerry devices. The protocol defines a routing layer that specifies the types of message contents allowed and the addressing information for the data. Gateways and routing components use this information to identify the type and source of the BlackBerry device data, and the appropriate destination service to route the data to.
GPS	Global Positioning System
GSA	General Services Administration
GSM	Global System for Mobile Communications
HMAC	keyed-hash message authentication code
HTTP	Hypertext Transfer Protocol over Secure Sockets Layer
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
initial key establishment protocol	The initial key establishment protocol is a BlackBerry proprietary protocol that the BlackBerry Enterprise Solution uses to generate the first device transport key for a BlackBerry device.
IT administration command	An IT administration command is a command that you can send over the wireless network to protect sensitive information on a BlackBerry device or delete all BlackBerry device data.
IP	Internet Protocol
IPsec	Internet Protocol Security
IT policy	An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager.
IT policy private key	The IT policy private key is a key that the BlackBerry Enterprise Server uses to sign an IT policy before the BlackBerry Enterprise Server sends the IT policy to a BlackBerry device.

IT policy public key	The IT policy public key is a key that a BlackBerry device uses to authenticate the IT policy that the BlackBerry Enterprise Server sends.
IT policy rule	An IT policy rule permits you to customize and control the actions that BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager can perform.
JSSE	Java Secure Socket Extension
KEA	Key Exchange Algorithm
key rollover protocol	The key rollover protocol is a BlackBerry proprietary protocol that the BlackBerry Enterprise Solution uses to generate subsequent device transport keys for a BlackBerry device.
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LEAP	Lightweight Extensible Authentication Protocol
MAC	message authentication code
MAPI	Messaging Application Programming Interface
MCEX	Mobile Commerce Extension
MD5	Message-Digest Algorithm, version 5
message keys	The message keys encrypt the data that is sent to and from a BlackBerry device.
messaging server	A messaging server sends and processes messages and provides collaboration services, such as updating and communicating calendar and address book information.
MIDP	Mobile Information Device Profile
MMS	Multimedia Messaging Service
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAT	network address translation
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
NTLM	NT LAN Manager
NV	nonvolatile
NV store	The NV store is a nonvolatile store that persists in application storage on a BlackBerry device. Only the operating system of the BlackBerry device can write to it. Third-party applications cannot write to the NV store.

OAEP	Optimal Asymmetric Encryption Padding
OCSP	Online Certificate Status Protocol
OFB	output feedback
PAC	proxy auto-configuration
PBX	Private Branch Exchange
PEAP	Protected Extensible Authentication Protocol
PFS	Perfect Forward Secrecy
persistent store in flash memory	The persistent store in flash memory stores data for a BlackBerry device. By default, third-party applications cannot access the persistent store. When it deletes all device data, the BlackBerry device deletes the data in the persistent store.
PGP/MIME	PGP Multipurpose Internet Mail Extensions
PIN	personal identification number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PMK	pairwise master key
POA	Post Office Agent
principal encryption key	The principal encryption key encrypts the device transport key when a BlackBerry device is locked if content protection is turned on.
PRNG	pseudorandom number generator
PSK	pre-shared key
PSS	Probabilistic Signature Scheme
PSK	pre-shared key
RC	Rivest's Cipher
remote password reset cryptographic protocol	The remote password reset cryptographic protocol is a BlackBerry proprietary protocol that permits you to reset the BlackBerry device password when content protection is turned on.
RFC	Request for Comments
BlackBerry signing authority system	
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RPC	remote procedure call

S/MIME	Secure Multipurpose Internet Mail Extensions
SEMA	Simple Electromagnetic Analysis
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPA	Simple Power Analysis
SPEKE	Simple Password-authenticated Exponential Key Exchange
SRP	Server Routing Protocol
SRP authentication	SRP authentication is an authentication method that the BlackBerry Enterprise Server and BlackBerry Infrastructure use to authenticate with each other.
SRP authentication key	The SRP authentication key is a 20-byte shared encryption key that the BlackBerry Enterprise Server and BlackBerry Infrastructure use to authenticate with each other during SRP authentication.
SRP ID	The SRP ID is a unique identifier for the BlackBerry Enterprise Server that the BlackBerry Enterprise Server uses to identify itself to the BlackBerry Infrastructure during SRP authentication.
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
Triple DES	Triple Data Encryption Standard
UID	unique identifier
UMA	Unlicensed Mobile Access
USB	Universal Serial Bus
VPN	virtual private network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	wireless local area network
WPA	Wi-Fi Protected Access

WTLS	Wireless Transport Layer Security

Legal notice

23

QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party

Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

Certain features outlined in this documentation require a minimum version of BlackBerry Enterprise Server, BlackBerry Desktop Software, and/or BlackBerry Device Software.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Certain features outlined in this documentation might require additional development or Third Party Products and Services for access to corporate applications.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada